

# MobileNext Broadband Gateway

## Configuration Guide

Release  
**12.1**



Published: 2013-07-16

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA  
408-745-2000  
[www.juniper.net](http://www.juniper.net)

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

#### *MobileNext Broadband Gateway Configuration Guide*

Revision History  
February 2013—R2 Junos OS 12.1W

The information in this document is current as of the date listed in the revision history.

#### YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

#### END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Abbreviated Table of Contents

	About This Guide .....	xxv
Part 1	Overview	
Chapter 1	System Architecture .....	3
Chapter 2	Mobile Network Architecture .....	23
Chapter 3	Getting Started with Mobile Networks .....	45
Part 2	System Configuration	
Chapter 4	Configuring Mobility on MX 3D Devices .....	67
Chapter 5	Configuring Redundancy on MX 3D Devices .....	77
Chapter 6	Configuring IP Reassembly .....	91
Part 3	APN Configuration	
Chapter 7	Configuring APNs .....	113
Part 4	Authorization, Addressing, and IPv6 Configuration	
Chapter 8	AAA Overview .....	167
Chapter 9	Configuring AAA .....	199
Chapter 10	Configuring Address Assignment .....	229
Chapter 11	Configuring DHCP .....	235
Chapter 12	Configuring IPv6 Stateless Address Autoconfiguration Parameters . . .	247
Part 5	Diameter Configuration	
Chapter 13	Diameter Overview .....	255
Chapter 14	Configuring Diameter .....	259
Part 6	GPRS Tunneling Protocol (GTP) Configuration	
Chapter 15	GTP Overview .....	287
Chapter 16	Configuring GTP .....	301
Part 7	Policy and Charging Enforcement Function Configuration	
Chapter 17	Policy and Charging Enforcement Function Overview .....	347
Chapter 18	Configuring Policy and Charging Enforcement Function .....	365

Part 8	Charging Configuration	
Chapter 19	Charging Overview .....	429
Chapter 20	Configuring Charging .....	443
Part 9	Quality of Service Configuration	
Chapter 21	Quality of Service Overview .....	499
Chapter 22	Configuring Quality of Service .....	515
Part 10	Maintenance	
Chapter 23	Maintenance Mode .....	591
Part 11	Configuration Examples	
Chapter 24	Mobility Configuration Examples .....	651
Part 12	Index	
	Index .....	737
	Index of Statements and Commands .....	751

# Table of Contents

	<b>About This Guide . . . . .</b>	<b>xxv</b>
	Junos Documentation and Release Notes . . . . .	xxv
	Objectives . . . . .	xxv
	Audience . . . . .	xxvi
	Supported Platforms . . . . .	xxvi
	Documentation Conventions . . . . .	xxvi
	Documentation Feedback . . . . .	xxviii
	Requesting Technical Support . . . . .	xxviii
	Self-Help Online Tools and Resources . . . . .	xxix
	Opening a Case with JTAC . . . . .	xxix
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>System Architecture . . . . .</b>	<b>3</b>
	Overview of Broadband Gateway System Architecture . . . . .	3
	Overview of Broadband Gateway System Control Packet Flow . . . . .	5
	Overview of Broadband Gateway Uplink Payload Packet Flow . . . . .	7
	Overview of Broadband Gateway Downlink Payload Packet Flow . . . . .	8
	Understanding the Broadband Gateway Software Data Path . . . . .	10
	Overview of Broadband Gateway as GGSN or P-GW . . . . .	11
	Understanding Mobile User Types . . . . .	12
	Serving Gateways and the MobileNext Broadband Gateway Overview . . . . .	12
	Overview of Standalone S-GW User Plane Packet Flow . . . . .	16
	MobileNext Broadband Gateway Configuration Overview . . . . .	17
	Overview of Collocated Gateways: Control Plane . . . . .	19
	Overview of Collocated Gateways: User Plane . . . . .	20
<b>Chapter 2</b>	<b>Mobile Network Architecture . . . . .</b>	<b>23</b>
	Overview of Mobile Networks . . . . .	23
	Overview of 3G Mobile Networks and the MobileNext Broadband Gateway . . . . .	25
	Overview of GGSN and P-GW . . . . .	26
	Overview of Packet Data Network Gateway Functions . . . . .	28
	Overview of the Evolved Packet Core . . . . .	30
	Overview of APNs . . . . .	32
	Overview of PDP Contexts and Bearers . . . . .	33
	Overview of GGSN and Broadband Gateway Deployment . . . . .	35
	Overview of 4G/LTE and Broadband Gateway Deployment . . . . .	36
	Overview of IPv6 and the Broadband Gateway . . . . .	38
	Serving Gateway and the S1 Interface Overview . . . . .	39
	Service Areas and Tracking Areas Overview . . . . .	40
	Serving Gateway Functions Overview . . . . .	41

<b>Chapter 3</b>	<b>Getting Started with Mobile Networks . . . . .</b>	<b>45</b>
	Configuring Broadband Gateway Home PLMNs and Gateways . . . . .	45
	Configuring Broadband Gateway Local Policies Application . . . . .	46
	Configuring Broadband Gateway Call Rate Statistics . . . . .	47
	Verifying the Gateway Configuration . . . . .	48
	Configuring General Gateway Trace Options . . . . .	49
	Configuring Mobile Options Trace Options . . . . .	51
	Configuring Resource Manager Trace Options . . . . .	52
	Configuring GGSN or P-GW Software Data Path Traceoptions . . . . .	55
	Configuring an S-GW on a Broadband Gateway . . . . .	57
	Configuring S-GW-Specific Profiles . . . . .	58
	Configuring S-GW Traceoptions . . . . .	59
	Configuring S-GW Software Data Path Traceoptions . . . . .	62
 <b>Part 2</b>	 <b>System Configuration</b>	
<b>Chapter 4</b>	<b>Configuring Mobility on MX 3D Devices . . . . .</b>	<b>67</b>
	MobileNext Broadband Gateway Chassis Overview . . . . .	68
	Session DPCs for Mobility . . . . .	69
	Overview of Mobility Interface Types . . . . .	69
	Configuring Session DPCs for Mobility . . . . .	70
	Configuring Interface DPCs or MPCs for User Mobility Traffic . . . . .	72
	Understanding the MobileNext Broadband Gateway Anchors . . . . .	73
	Configuring Anchor Session DPCs and PFEs . . . . .	75
	Verifying the MobileNext Broadband Gateway Chassis Configuration . . . . .	76
 <b>Chapter 5</b>	 <b>Configuring Redundancy on MX 3D Devices . . . . .</b>	 <b>77</b>
	Broadband Gateway Redundancy Overview . . . . .	78
	Routing Engine Redundancy . . . . .	78
	Session DPC Redundancy . . . . .	79
	Interface Redundancy . . . . .	80
	Configuring Session DPC Redundancy . . . . .	80
	Configuring Interface Redundancy . . . . .	82
	Understanding the Broadband Gateway Anchor Failover Behavior . . . . .	84
	Example: Configuring Broadband Gateway Redundancy . . . . .	86
 <b>Chapter 6</b>	 <b>Configuring IP Reassembly . . . . .</b>	 <b>91</b>
	IP Packet Fragment Reassembly for Mobility Overview . . . . .	91
	Understanding Default IP Fragment Handling . . . . .	94
	Configuring IP Inline Reassembly for Mobility . . . . .	96
	Configuring Software-Based Fragment Reassembly Parameters . . . . .	98
	Example: Configuring Inline IP Packet Fragment Reassembly . . . . .	99
	Example: Configuring Software-Based IP Reassembly Parameters . . . . .	107
 <b>Part 3</b>	 <b>APN Configuration</b>	
<b>Chapter 7</b>	<b>Configuring APNs . . . . .</b>	<b>113</b>
	Configuring APNs on the MobileNext Broadband Gateway Overview . . . . .	113
	General APN Parameters . . . . .	114
	Restriction Value . . . . .	114

User Options . . . . .	115
Address Assignment . . . . .	115
Anchor DPC or MPC Failure Behavior . . . . .	115
Charging Profiles . . . . .	115
User-Session Routing Overview . . . . .	115
Configuring General APN Parameters on the Broadband Gateway . . . . .	117
Configuring the APN Name, Interface, and Type . . . . .	117
Configuring Servers for an APN . . . . .	118
Configuring APN Timers . . . . .	119
Configuring Miscellaneous APN Parameters . . . . .	119
Configuring the Restriction Value on a Broadband Gateway APN . . . . .	121
Configuring Address Assignment on a Broadband Gateway APN . . . . .	122
Configuring Charging, Local Policy, and Policy and Charging Enforcement	
Function Profiles on a Broadband Gateway APN . . . . .	131
Configuring Mobile Interfaces for APNs . . . . .	133
Configuring Mobile Interface to APN Associations in VRFs . . . . .	134
Configuring APN Service Selection on a Broadband Gateway . . . . .	135
Configuring User Options on a Broadband Gateway APN . . . . .	141
Example: Configuring Broadband Gateway APNs . . . . .	143
Networks Behind the Mobile Device Overview . . . . .	146
Configuring the Networks Behind the Mobile Equipment Feature . . . . .	148
Example: Configuring the Networks Behind the Mobile Device Feature . . . . .	150
HTTP Header Enrichment Overview . . . . .	153
Configuring HTTP Header Enrichment . . . . .	154
Example: Configuring HTTP Header Enrichment . . . . .	157

## Part 4

### Chapter 8

## Authorization, Addressing, and IPv6 Configuration

<b>AAA Overview . . . . .</b>	<b>167</b>
Overview of AAA on the Broadband Gateway . . . . .	167
Authentication . . . . .	167
Accounting . . . . .	168
APN-Specific AAA Settings . . . . .	169
RADIUS-Initiated Dynamic Requests . . . . .	169
Support for RADIUS Attributes, Juniper Networks VSAs, and 3GPP VSAs . . . . .	169
Scalability and Redundancy . . . . .	170
Scalability . . . . .	170
Redundancy . . . . .	170
Network Elements . . . . .	171
Load Balancing Within Network Elements . . . . .	171
Server Priority . . . . .	171
Dead Server Detection . . . . .	171
Maximum Pending Requests for a Network Element . . . . .	171
Network Element Groups . . . . .	172
AAA Profiles . . . . .	172
Authentication Options . . . . .	172
Accounting Options . . . . .	173
RADIUS Attributes to Ignore or Exclude . . . . .	173

	RADIUS Options . . . . .	173
	Supported Attributes in Access-Request Messages . . . . .	174
	RADIUS IETF Attributes Supported in Access-Request Messages . . . . .	174
	3GPP VSAs Supported in Access-Request Messages . . . . .	176
	Supported Attributes in Access-Accept Messages . . . . .	179
	RADIUS IETF Attributes Supported in Access-Accept Messages . . . . .	179
	3GPP VSAs Supported in Access-Accept Messages . . . . .	181
	Juniper Networks VSAs Supported in Access-Accept Messages . . . . .	181
	Supported Attributes in Accounting Start Messages . . . . .	182
	RADIUS IETF Attributes Supported in Accounting Start Messages . . . . .	182
	3GPP VSAs Supported in Accounting Start Messages . . . . .	183
	Supported Attributes in Accounting Interim Update Messages . . . . .	186
	RADIUS IETF Attributes Supported in Interim-Update Messages . . . . .	186
	3GPP VSAs Supported in Interim-Update Messages . . . . .	188
	Supported Attributes in Accounting Stop Messages . . . . .	190
	RADIUS IETF Attributes Supported in Accounting Stop Messages . . . . .	190
	3GPP VSAs Supported in Accounting Stop Messages . . . . .	193
	Supported Attributes in Accounting On Messages . . . . .	195
	RADIUS IETF Attributes Supported in Accounting On Messages . . . . .	195
	Supported Attributes in Disconnect Request Messages . . . . .	196
	RADIUS IETF Attributes Supported in Disconnect Request Messages . . . . .	196
	3GPP VSAs Supported in Disconnect Request Messages . . . . .	196
	Supported Attributes in Change of Authorization (CoA) Messages . . . . .	197
	RADIUS IETF Attributes Supported in CoA Messages . . . . .	197
	3GPP VSAs Supported in CoA Messages . . . . .	198
<b>Chapter 9</b>	<b>Configuring AAA . . . . .</b>	<b>199</b>
	Configuring AAA on the Broadband Gateway . . . . .	199
	Configuring Interaction Between the Broadband Gateway and RADIUS Servers . . . . .	200
	Configuring RADIUS-Initiated Dynamic Request Support . . . . .	201
	Configuring Dead Server Detection . . . . .	202
	Configuring Network Elements . . . . .	203
	Configuring Network Element Groups . . . . .	204
	Configuring an AAA Profile . . . . .	204
	Configuring Authentication Settings in an AAA Profile . . . . .	205
	Configuring Accounting Settings in an AAA Profile . . . . .	205
	Configuring RADIUS Attribute Usage for an AAA Profile . . . . .	207
	Specifying RADIUS Options in an AAA Profile . . . . .	210
	Applying an AAA Profile to an APN . . . . .	211
	Enabling Address Assignment by the RADIUS Server . . . . .	211
	Configuring AAA-Assigned Addresses to Override Locally or DHCP-Assigned Addresses . . . . .	212
	Configuring the Broadband Gateway to Wait for an Accounting Response . . . . .	212
	Example: Configuring AAA on the Broadband Gateway . . . . .	213



<b>Chapter 10</b>	<b>Configuring Address Assignment . . . . .</b>	<b>229</b>
	Overview of Mobile Pools and Mobile Pool Groups for the Broadband Gateway . . . . .	229
	Configuring Mobile Pools and Mobile Pool Groups on the Broadband Gateway . . . . .	230
<b>Chapter 11</b>	<b>Configuring DHCP . . . . .</b>	<b>235</b>
	DHCP Overview . . . . .	235
	Understanding DHCP Proxy Clients . . . . .	236
	Configuring DHCPv4 Proxy Client Profiles . . . . .	237
	Configuring DHCPv6 Proxy Client Profiles . . . . .	240
	Configuring the DHCP Proxy Client on the Broadband Gateway . . . . .	242
	Configuring DHCP Traceoptions on the Broadband Gateway . . . . .	242
	Enabling DHCP on a Broadband Gateway APN . . . . .	245
<b>Chapter 12</b>	<b>Configuring IPv6 Stateless Address Autoconfiguration Parameters . . . . .</b>	<b>247</b>
	Understanding IPv6 Stateless Address Autoconfiguration Parameters . . . . .	247
	Configuring IPv6 Router Advertisement Parameters . . . . .	248
	Example: Configuring IPv6 Router Advertisement Parameters . . . . .	250
<b>Part 5</b>	<b>Diameter Configuration</b>	
<b>Chapter 13</b>	<b>Diameter Overview . . . . .</b>	<b>255</b>
	Diameter Base Protocol Overview . . . . .	255
	Overview of Diameter Profiles . . . . .	256
<b>Chapter 14</b>	<b>Configuring Diameter . . . . .</b>	<b>259</b>
	Configuring Diameter . . . . .	259
	Configuring the Origin Attributes of the Diameter Instance . . . . .	260
	Configuring the Diameter Transport . . . . .	260
	Configuring Diameter Peers . . . . .	261
	Configuring Diameter Network Elements . . . . .	263
	Configuring Advertisements in Diameter Messages . . . . .	263
	Configuring Parameters for Diameter Applications . . . . .	264
	Tracing Diameter Operations . . . . .	264
	Configuring the Trace Log Filename . . . . .	265
	Configuring the Tracing Flags . . . . .	265
	Configuring Tracing for a Diameter Peer . . . . .	266
	Configuring Diameter Profiles . . . . .	266
	Configuring Diameter AVPs for Gy Applications . . . . .	267
	Configuring Diameter AVPs for Gx Applications . . . . .	269
	Configuring Diameter Bindings . . . . .	271
	Example: Configuring Diameter . . . . .	271
	Example: Configuring Diameter for Load Balancing . . . . .	279
<b>Part 6</b>	<b>GPRS Tunneling Protocol (GTP) Configuration</b>	
<b>Chapter 15</b>	<b>GTP Overview . . . . .</b>	<b>287</b>
	GTP Versions and GPRS Interfaces Overview . . . . .	287
	GPRS Tunneling Protocol (GTP) Overview . . . . .	289

	GTP Path Management Overview . . . . .	290
	Default Path Management Configuration . . . . .	290
	GTP Version Support for Echo Requests and Echo Responses . . . . .	291
	Understanding Path Management . . . . .	291
	Successful Echo-Request Sequence for Path Management . . . . .	291
	Failed Echo Request Sequence for Path Management . . . . .	292
	GTP Tunnel Management Overview . . . . .	294
	GTP Tunnel Management Functions . . . . .	294
	Default Tunnel Management Configuration . . . . .	294
	GTP Version Support for Tunnel Management Requests and Responses . . . . .	294
	Understanding Tunnel Management . . . . .	295
	Successful Create Request Sequence for Tunnel Management . . . . .	295
	Successful Update/Delete Request Sequence for Tunnel Management . . . . .	295
	Failed Update/Delete Request Sequence for Tunnel Management . . . . .	296
	Restart Counters Overview . . . . .	297
	Understanding CSID Signaling . . . . .	298
	Understanding Tunnel Endpoint Identifiers . . . . .	299
	Understanding GTP-U Error Data Path . . . . .	300
<b>Chapter 16</b>	<b>Configuring GTP . . . . .</b>	<b>301</b>
	Configuring GTP Services Overview . . . . .	302
	GTP-C and GTP-U Path Management . . . . .	302
	Configuring GTP Services at Different Levels on a Broadband Gateway . . . . .	302
	GTP Services Default Settings . . . . .	303
	GTP Version Support . . . . .	304
	Configuring a Loopback Interface for Transport of GTP Packets . . . . .	304
	Configuring GTP Services on a Broadband Gateway . . . . .	305
	Configuring GTP Services on the Control Plane . . . . .	306
	Configuring GTP Services on the Data Plane . . . . .	308
	Configuring GTP Services on the S5 Interface . . . . .	309
	Configuring GTP Services on the S8 Interface . . . . .	310
	Configuring GTP Services on the Gn Interface . . . . .	312
	Configuring GTP Services on the Gp Interface . . . . .	314
	Configuring GTP Services When the S5 and S8 Interfaces Are in Different VRFs . . . . .	315
	Configuring GTP Services When the S5 and S8 Interfaces Are in the Same VRF . . . . .	317
	Configuring GTP Services When 3GPP Interfaces Are in Different VRFs . . . . .	318
	Configuring GTP Services on a GGSN Broadband Gateway . . . . .	320
	Configuring GTP Services on a Peer Group . . . . .	321
	Disabling Path Management on a Broadband Gateway or Peer Group . . . . .	323
	Configuring GTP Trace Options . . . . .	323
	Configuring General GTP Service on the S-GW . . . . .	325
	Configuring GTP-C Services on the S11 Interface . . . . .	328
	Configuring GTP-U Services on the S12 Interface . . . . .	330
	Configuring GTP Services on the S1-U Interface . . . . .	332
	Configuring GTP Services on the S4 Interface . . . . .	333
	Configuring GTP Services on the S-GW When the S4 and S5 Interfaces Are in the Same VRF . . . . .	335

	Configuring GTP Services on the S-GW When Interfaces are in Different VRFs . . . . .	337
	Configuring S-GW GTP Traceoptions . . . . .	338
	Example: Configuring GTP for the S-GW When Interfaces Are in different VRFs . . . . .	340
<b>Part 7</b>	<b>Policy and Charging Enforcement Function Configuration</b>	
<b>Chapter 17</b>	<b>Policy and Charging Enforcement Function Overview . . . . .</b>	<b>347</b>
	Policy and Charging Enforcement Function Overview . . . . .	347
	Policy and Charging Control Rules Overview . . . . .	349
	Understanding Service Data Flow Filters . . . . .	349
	Policy and Charging Control . . . . .	351
	PCC Rules Under Static Policy Control . . . . .	352
	PCC Rules Under Dynamic Policy Control . . . . .	352
	Static-Gx Rules . . . . .	353
	Policing of Subscriber Traffic . . . . .	353
	Application-Aware Policy and Charging Control Rules Overview . . . . .	353
	Understanding Application-Aware PCEF Services on the Broadband Gateway . . . . .	354
	Use Case for Application-Aware PCEF Service . . . . .	354
	Junos OS Services Package Requirements for Application-Aware PCEF . . . . .	355
	APPID Feature Overview . . . . .	355
	Application Tracking (AppTrack) . . . . .	356
	Custom Application Signatures . . . . .	356
	Signature Groups . . . . .	357
	Heuristics-Based Detection . . . . .	358
	Nested Application Identification . . . . .	358
	Understanding How Dynamic and Static Policy and Charging Control Rules Are Provisioned . . . . .	359
	Understanding How Rules Are Provisioned on the Gx Interface . . . . .	359
	Provisioning of Dynamic Policies . . . . .	359
	Provisioning of Predefined Static Policies . . . . .	361
	Bearer Binding Overview . . . . .	361
	Understanding Event Triggers . . . . .	363
	Implicit Event Triggers . . . . .	363
	Configurable PCEF-Enabled Event Triggers . . . . .	363
<b>Chapter 18</b>	<b>Configuring Policy and Charging Enforcement Function . . . . .</b>	<b>365</b>
	Configuring Policy and Charging Enforcement Function Services for Application-Aware Traffic . . . . .	365
	Configuring Service Data Flow Filters (Flow Identifiers) . . . . .	367
	Configuring Policy and Charging Control Action Profiles . . . . .	369
	Configuring Layer 3 and Layer 4 Policy and Charging Control Rules . . . . .	370
	Configuring Application-Aware Policy and Charging Control Rules . . . . .	371
	Configuring a Policy and Charging Control Rulebase . . . . .	372
	Configuring Event Trigger Profiles . . . . .	373
	Configuring a Policy and Charging Enforcement Function Profile for Dynamic Policies . . . . .	375

	Configuring a Policy and Charging Enforcement Function Profile for Static Policies . . . . .	377
	Tracing PCEF Operations . . . . .	378
	Example: Configuring Policy and Charging Enforcement Function With Layer 3 and Layer 4 Policy and Charging Control Rules . . . . .	379
	Example: Configuring Policy and Charging Enforcement Function with Application-Aware Policy and Charging Control Rules . . . . .	397
<b>Part 8</b>	<b>Charging Configuration</b>	
<b>Chapter 19</b>	<b>Charging Overview . . . . .</b>	<b>429</b>
	Charging Overview . . . . .	429
	Charging in Mobile Networks . . . . .	430
	Charging with Data Records (Offline Charging) . . . . .	430
	Charging in Real Time (Online Charging) . . . . .	431
	Offline Charging Overview . . . . .	431
	Online Charging Overview . . . . .	433
	Charging Data Records . . . . .	434
	Information Collection and CDR Generation . . . . .	436
	CDR Delivery . . . . .	437
	Charging Profiles . . . . .	438
	Charging Profile Selection Process . . . . .	439
	Advice of Charge Overview . . . . .	440
	Advice of Charge on the Broadband Gateway . . . . .	440
	Service Sets and Service Filters for Advice of Charge Overview . . . . .	441
<b>Chapter 20</b>	<b>Configuring Charging . . . . .</b>	<b>443</b>
	Configuring Offline Charging . . . . .	443
	Configuring S-GW-Specific Charging Parameters . . . . .	444
	Configuring S-GW Global Charging Profiles and Selection Order . . . . .	446
	Configuring S-GW Charging Traceoptions . . . . .	448
	Configuring S-GW Local Persistent Storage Traceoptions . . . . .	451
	Configuring GTP Prime for Charging . . . . .	453
	Configuring GTP Prime for Transferring CDRs . . . . .	453
	Configuring GTP Prime Peers . . . . .	454
	Configuring Persistent Storage . . . . .	455
	Configuring Local Persistent Storage . . . . .	455
	Tracing Persistent Storage Operations . . . . .	456
	Configuring the Solid State Disk for Persistent Storage . . . . .	457
	Initializing the Solid State Disk for Persistent Storage . . . . .	457
	Ejecting the Solid State Disk . . . . .	458
	Installing the Solid State Disk . . . . .	458
	Configuring Transport Profiles for Offline Charging . . . . .	459
	Configuring Charging Trigger Events for Offline Charging . . . . .	462
	Configuring CDR Attributes . . . . .	464
	Configuring Charging Profiles . . . . .	467
	Configuring Charging Profiles for APNs . . . . .	469
	Tracing Charging Operations . . . . .	470
	Configuring the Trace Log Filename . . . . .	471
	Configuring the Tracing Flags . . . . .	471

	Configuring Online Charging . . . . .	472
	Configuring Transport Profiles for Online Charging . . . . .	473
	Configuring Charging Trigger Events for Online Charging . . . . .	476
	Configuring Credit Control Failure Handling Parameters . . . . .	476
	Configuring Miscellaneous Online Charging Trigger Events . . . . .	480
	Verifying and Managing the Charging Configuration . . . . .	484
	Example: Configuring Online Charging . . . . .	486
	Configuring Service Sets and Service Filters for Advice of Charge . . . . .	495
<b>Part 9</b>	<b>Quality of Service Configuration</b>	
<b>Chapter 21</b>	<b>Quality of Service Overview . . . . .</b>	<b>499</b>
	Quality of Service Overview . . . . .	499
	Initial QoS . . . . .	500
	Differentiated Services . . . . .	500
	QoS Parameters in 3G Networks . . . . .	500
	Default Conversion of (3G) Traffic Classes to (4G) QoS Class Identifiers on the Broadband Gateway . . . . .	502
	QoS Parameters in 4G Networks . . . . .	503
	Aggregate Maximum Bit Rate . . . . .	504
	Allocation and Retention Priority . . . . .	504
	Preemption . . . . .	505
	Call Admission Control Overview . . . . .	506
	Enforcing Call Admission Control . . . . .	506
	Managing Bandwidth . . . . .	506
	Managing the Number of Bearers . . . . .	507
	Managing Resource Thresholds . . . . .	507
	Default Resource Threshold Settings . . . . .	507
	Class of Service (CoS) Policy Profile Overview . . . . .	508
	Policing Subscriber Traffic on the Broadband Gateway Overview . . . . .	509
	Applying Rewrite Rules on Mobile Interfaces Overview . . . . .	510
	Understanding Upstream and Downstream Processing of ToS Values in GTP-U Packets . . . . .	511
	Processing of ToS Values for Upstream Subscriber Packets . . . . .	511
	Processing of ToS Values for Downstream Subscriber Packets . . . . .	512
	Understanding How NQN and Upgrade Flags in PDP Contexts Affect QoS Upgrade Behavior . . . . .	513
<b>Chapter 22</b>	<b>Configuring Quality of Service . . . . .</b>	<b>515</b>
	Configuring QoS on the Broadband Gateway Overview . . . . .	516
	Configuring the Maximum Number of Bearers . . . . .	517
	Configuring Bandwidth Pools . . . . .	518
	Configuring Preemption for Call Admission Control . . . . .	519
	Configuring Resource Thresholds for 3G and 4G Networks . . . . .	520
	Configuring a Classifier Profile for 3G and 4G Networks . . . . .	521
	Configuring a CoS Policy Profile for 4G Networks . . . . .	523
	Configuring a CoS Policy Profile for 3G Networks . . . . .	526
	Configuring a CoS Policy Profile for 3G and 4G Networks . . . . .	531
	Configuring a Local Policy . . . . .	537
	Applying a Local Policy . . . . .	538

	Configuring Ingress Rewrite Rules for a Mobile Interface . . . . .	539
	Configuring Egress Rewrite Rules for a Mobile Interface . . . . .	539
	Applying Ingress Rewrite Rules to a Mobile Interface . . . . .	540
	Applying Egress Rewrite Rules to Mobile Interfaces . . . . .	541
	Example: Configuring Quality of Service on GGSN/P-GW . . . . .	542
	Verifying Quality of Service . . . . .	579
	Configuring S-GW-Specific CAC Parameters . . . . .	581
	Example: Configuring QoS and CAC on a S-GW . . . . .	582
<b>Part 10</b>	<b>Maintenance</b>	
<b>Chapter 23</b>	<b>Maintenance Mode . . . . .</b>	<b>591</b>
	Mobility Maintenance Mode Overview . . . . .	592
	Changing a GTP Interface . . . . .	593
	Deleting a GTP Interface . . . . .	595
	Modifying an Access Point Name . . . . .	596
	Configuring the Mobile Interface of an Access Point Name . . . . .	598
	Deleting an Access Point Name . . . . .	599
	Changing a Charging Profile . . . . .	601
	Changing a Transport Profile . . . . .	603
	Deleting a Charging Profile . . . . .	605
	Deleting a Transport Profile . . . . .	606
	Changing Address Attributes in the Mobile Address Pool . . . . .	607
	Deleting a Mobile Address Pool . . . . .	609
	Deleting a Session PIC . . . . .	610
	Deleting a Services PIC . . . . .	612
	Changing AMS Interface Parameters . . . . .	614
	Changing Gateway Parameters with Maintenance Mode . . . . .	617
	Example: Changing Access Point Name Values . . . . .	619
	Example: Deleting an APN . . . . .	620
	Example: Changing a Charging Profile . . . . .	622
	Example: Changing a Transport Profile . . . . .	624
	Example: Changing Mobility Pool Attributes . . . . .	625
	Example: Deleting a Mobility Address Pool . . . . .	631
	Example: Modifying Mobile Interface Parameters . . . . .	633
	Example: Deleting a Session PIC . . . . .	636
	Example: Deleting a Services PIC . . . . .	640
	Example: Changing an AMS Interface . . . . .	643
<b>Part 11</b>	<b>Configuration Examples</b>	
<b>Chapter 24</b>	<b>Mobility Configuration Examples . . . . .</b>	<b>651</b>
	Example: Simple Unified Edge Configuration . . . . .	651
	Example: Configuring MobileNext Broadband Gateway . . . . .	658
	Example: Configuring MobileNext Broadband Gateway with Provider Edge Functionality . . . . .	689
	Example: Configuring NAT . . . . .	698
	Example: Configuring a Standalone S-GW . . . . .	702
	Example: Configuring a Collocated P-GW and S-GW . . . . .	708

	Example: Configuring a Multigateway P-GW and S-GW . . . . .	719
Part 12	Index	
	Index . . . . .	737
	Index of Statements and Commands . . . . .	751





# List of Figures

<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>System Architecture</b>	<b>3</b>
	Figure 1: The Broadband Gateway System Architecture	4
	Figure 2: Broadband Gateway GTP Signaling Packet Flow	5
	Figure 3: Broadband Gateway Uplink User Packet Flow	7
	Figure 4: Broadband Gateway Downlink User Packet Flow	8
	Figure 5: GTP-C Handling	10
	Figure 6: S-GW Interfaces on the Broadband Gateway	13
	Figure 7: S-GW and the S1 and X2 Interfaces	15
	Figure 8: GTP-U Packet Flow Through Standalone S-GW	16
	Figure 9: Collocated Gateways S-GW and P-GW Resources and Load Balancing	17
	Figure 10: Collocated S-GW and P-GW Control Packet Flow	19
	Figure 11: Collocated S-GW and P-GW User Packet Flow	20
<b>Chapter 2</b>	<b>Mobile Network Architecture</b>	<b>23</b>
	Figure 12: 3G Mobile Network Architecture	25
	Figure 13: 4G/LTE Mobile Network Basic Components	27
	Figure 14: Packet Data Network Gateway Functions	28
	Figure 15: Major Components of the Evolved Packet Core	30
	Figure 16: APNs and the P-GW	32
	Figure 17: Bearers, Gateways, and Packet Networks	34
	Figure 18: The GGSN in a 3G Network	35
	Figure 19: LTE Network Deployment Scenario	37
	Figure 20: S1 Interface Is Many-to-Many	39
	Figure 21: Tracking Areas and the S1 Interface	40
	Figure 22: S-GW Functions	42
<b>Part 2</b>	<b>System Configuration</b>	
<b>Chapter 4</b>	<b>Configuring Mobility on MX 3D Devices</b>	<b>67</b>
	Figure 23: Session DPCs and Interfaces on the Broadband Gateway	68
	Figure 24: Upstream GTP-U Traffic	74
	Figure 25: Downstream GTP-U Traffic	74
<b>Chapter 5</b>	<b>Configuring Redundancy on MX 3D Devices</b>	<b>77</b>
	Figure 26: Redundancy Available on the Broadband Gateway	78
	Figure 27: Control Plane Anchor Operation Before Failure	84
	Figure 28: Control Plane Anchor Operation After Failure	85
	Figure 29: Pre- and Post-Failure PFE Datapaths	85
	Figure 30: Redundancy Example for the Broadband Gateway	87

<b>Chapter 6</b>	<b>Configuring IP Reassembly . . . . .</b>	<b>91</b>
	Figure 31: Fragmented Packet Requiring Reassembly . . . . .	92
	Figure 32: A GTP-U Header Causing Fragmentation . . . . .	93
	Figure 33: Fragmented Packet Requiring Reassembly . . . . .	100
	Figure 34: A GTP-U Header Causing Fragmentation . . . . .	102
<b>Part 3</b>	<b>APN Configuration</b>	
<b>Chapter 7</b>	<b>Configuring APNs . . . . .</b>	<b>113</b>
	Figure 35: APNs and P-GWs in the 4G Architecture . . . . .	114
	Figure 36: APNs Connect Mobile Devices to IP Networks Through a P-GW . . . . .	143
	Figure 37: Network That Is Behind the Mobile Device and the P-GW . . . . .	147
<b>Part 4</b>	<b>Authorization, Addressing, and IPv6 Configuration</b>	
<b>Chapter 11</b>	<b>Configuring DHCP . . . . .</b>	<b>235</b>
	Figure 38: DHCP Proxy Client Architecture . . . . .	236
<b>Part 6</b>	<b>GPRS Tunneling Protocol (GTP) Configuration</b>	
<b>Chapter 15</b>	<b>GTP Overview . . . . .</b>	<b>287</b>
	Figure 39: GTP Versions Supported on a MobileNext Broadband Gateway . . . . .	287
	Figure 40: GTP-C Versions Supported for 3G/4G Network Interfaces . . . . .	288
	Figure 41: Successful Echo-Request Sequence for Path Management . . . . .	292
	Figure 42: Failed Echo-Request Sequence for Path Management . . . . .	293
	Figure 43: Successful Create Request Sequence for Tunnel Management . . . . .	295
	Figure 44: Successful Update/Delete Request Sequence for Tunnel Management . . . . .	296
	Figure 45: Failed Update/Delete Request Sequence for Tunnel Management . . . . .	297
	Figure 46: GTP-C Performs Signaling Between the Serving Gateway and Packet Data Network Gateway . . . . .	299
<b>Part 7</b>	<b>Policy and Charging Enforcement Function Configuration</b>	
<b>Chapter 17</b>	<b>Policy and Charging Enforcement Function Overview . . . . .</b>	<b>347</b>
	Figure 47: Architecture for Policy and Charging Enforcement Function . . . . .	348
	Figure 48: Service Data Flow Filtering of Downlink IP Packets . . . . .	351
	Figure 49: Message Flow for Push Mode . . . . .	360
	Figure 50: Message Flow for Pull Mode . . . . .	361
<b>Chapter 18</b>	<b>Configuring Policy and Charging Enforcement Function . . . . .</b>	<b>365</b>
	Figure 51: Architecture for Policy and Charging Enforcement Function . . . . .	380
	Figure 52: Architecture for Policy and Charging Enforcement Function . . . . .	398
<b>Part 8</b>	<b>Charging Configuration</b>	
<b>Chapter 19</b>	<b>Charging Overview . . . . .</b>	<b>429</b>
	Figure 53: Simple Charging Topology . . . . .	432
	Figure 54: General Architecture for Charging . . . . .	434
	Figure 55: System Architecture for Advice of Charge and Top-Up . . . . .	440

<b>Chapter 20</b>	<b>Configuring Charging . . . . .</b>	<b>443</b>
	Figure 56: Architecture for Online Charging . . . . .	487
<b>Part 9</b>	<b>Quality of Service Configuration</b>	
<b>Chapter 21</b>	<b>Quality of Service Overview . . . . .</b>	<b>499</b>
	Figure 57: Key QoS Parameters for PDP Context Requests . . . . .	501
	Figure 58: Key QoS Parameters for 4G Default Bearer Requests . . . . .	504
	Figure 59: QoS Negotiation Behavior for PDP Contexts with NQN and Upgrade Flags . . . . .	513



# List of Tables

	<b>About This Guide</b> . . . . .	<b>xxv</b>
	Table 1: Notice Icons . . . . .	xxvii
	Table 2: Text and Syntax Conventions . . . . .	xxvii
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 3</b>	<b>Getting Started with Mobile Networks</b> . . . . .	<b>45</b>
	Table 3: General Gateway Trace Flags . . . . .	49
	Table 4: Trace Levels . . . . .	49
	Table 5: Mobile Options Trace Flags . . . . .	51
	Table 6: Resource Management Server Trace Flags . . . . .	52
	Table 7: Resource Management Client Trace Flags . . . . .	53
	Table 8: Trace Levels . . . . .	53
	Table 9: Trace Flags . . . . .	55
	Table 10: Trace Levels . . . . .	55
	Table 11: S-GW Trace Flags . . . . .	59
	Table 12: S-GW Trace Levels . . . . .	60
	Table 13: S-GW Data Path Trace Flags . . . . .	62
	Table 14: S-GW Datapath Trace Levels . . . . .	62
<b>Part 3</b>	<b>APN Configuration</b>	
<b>Chapter 7</b>	<b>Configuring APNs</b> . . . . .	<b>113</b>
	Table 15: APN Restriction Values . . . . .	121
<b>Part 4</b>	<b>Authorization, Addressing, and IPv6 Configuration</b>	
<b>Chapter 8</b>	<b>AAA Overview</b> . . . . .	<b>167</b>
	Table 16: RADIUS IETF Attributes Supported in Access-Request Messages . . . . .	175
	Table 17: 3GPP VSAs Supported in Access-Request Messages . . . . .	176
	Table 18: RADIUS IETF Attributes Supported in Access-Accept Messages . . . . .	179
	Table 19: 3GPP VSAs Supported in Access-Accept Messages . . . . .	181
	Table 20: Juniper VSAs Supported in Access-Accept Messages . . . . .	181
	Table 21: RADIUS IETF Attributes Supported in Accounting Start Messages . . . . .	182
	Table 22: 3GPP VSAs Supported in Accounting Start Messages . . . . .	184
	Table 23: RADIUS IETF Attributes Supported in Accounting Interim-Update Messages . . . . .	186
	Table 24: 3GPP VSAs Supported in Accounting Interim-Update Messages . . . . .	188
	Table 25: RADIUS IETF Attributes Supported in Accounting Stop Messages . . . . .	191
	Table 26: 3GPP VSAs Supported in Accounting Stop Messages . . . . .	193
	Table 27: RADIUS IETF Attributes Supported in Accounting On Messages . . . . .	195

	Table 28: RADIUS IETF Attributes Supported in Disconnect Request Messages . . . . .	196
	Table 29: 3GPP VSAs Supported in Disconnect Request Messages . . . . .	197
	Table 30: RADIUS IETF Attributes Supported in CoA Messages . . . . .	197
	Table 31: 3GPP VSAs Supported in CoA Messages . . . . .	198
<b>Chapter 9</b>	<b>Configuring AAA . . . . .</b>	<b>199</b>
	Table 32: Events You Can Exclude from Triggering Interim-Update Messages . .	206
	Table 33: RADIUS Attributes the Broadband Gateway Can Ignore in Accept-Accept Messages . . . . .	207
	Table 34: RADIUS Attributes the Broadband Gateway Can Exclude from RADIUS Messages . . . . .	208
	Table 35: 3GPP VSAs That Can Be Excluded from RADIUS Messages . . . . .	209
<b>Chapter 11</b>	<b>Configuring DHCP . . . . .</b>	<b>235</b>
	Table 36: DHCP Trace Flags . . . . .	242
<b>Part 5</b>	<b>Diameter Configuration</b>	
<b>Chapter 14</b>	<b>Configuring Diameter . . . . .</b>	<b>259</b>
	Table 37: Diameter Tracing Flags . . . . .	266
	Table 38: Diameter AVP Exclusions for Gy Applications . . . . .	268
	Table 39: Diameter AVP Inclusions for Gy Applications . . . . .	269
	Table 40: Diameter AVP Exclusions for Gx Applications . . . . .	270
	Table 41: Diameter AVP Inclusions for Gx Applications . . . . .	270
<b>Part 6</b>	<b>GPRS Tunneling Protocol (GTP) Configuration</b>	
<b>Chapter 16</b>	<b>Configuring GTP . . . . .</b>	<b>301</b>
	Table 42: Trace Flags . . . . .	323
	Table 43: Trace Levels . . . . .	324
	Table 44: S-GW GTP Trace Flags . . . . .	338
	Table 45: S-GW GTP Trace Levels . . . . .	339
	Table 46: Components of the Broadband Gateway . . . . .	341
<b>Part 8</b>	<b>Charging Configuration</b>	
<b>Chapter 20</b>	<b>Configuring Charging . . . . .</b>	<b>443</b>
	Table 47: S-GW Charging Trace Flags . . . . .	448
	Table 48: S-GW Charging Trace Levels . . . . .	449
	Table 49: S-GW Local Persistent Storage Trace Flags . . . . .	451
	Table 50: S-GW Local Persistent Storage Trace Levels . . . . .	451
	Table 51: Bearer Information Changes . . . . .	463
	Table 52: Attribute Exclusions . . . . .	465
	Table 53: Charging Tracing Flags . . . . .	471
<b>Part 9</b>	<b>Quality of Service Configuration</b>	
<b>Chapter 21</b>	<b>Quality of Service Overview . . . . .</b>	<b>499</b>
	Table 54: Traffic Classes for 3G Networks . . . . .	501
	Table 55: Mapping of Traffic Classes to Qos Class Identifiers . . . . .	502

	Table 56: QoS Class Identifiers for 4G Networks . . . . .	503
	Table 57: Conversion of GTPv1 Pre-Release 9 ARP Values to Release 9 ARP Values . . . . .	504
	Table 58: Mapping of Release 9 ARP Values to Pre-Release 9 ARP Values . . .	505
<b>Chapter 22</b>	<b>Configuring Quality of Service . . . . .</b>	<b>515</b>
	Table 59: Mapping of EPS Bearer ARP to Release 99 Bearer Parameter ARP . .	520
<b>Part 11</b>	<b>Configuration Examples</b>	
<b>Chapter 24</b>	<b>Mobility Configuration Examples . . . . .</b>	<b>651</b>
	Table 60: Unified Edge — Simple Configuration . . . . .	652
	Table 61: Components of the Broadband Gateway . . . . .	659
	Table 62: Components of the Broadband Gateway . . . . .	690





# About This Guide

- Junos Documentation and Release Notes on page xxv
- Objectives on page xxv
- Audience on page xxvi
- Supported Platforms on page xxvi
- Documentation Conventions on page xxvi
- Documentation Feedback on page xxviii
- Requesting Technical Support on page xxviii

## Junos Documentation and Release Notes

---

For a list of related Junos documentation, see  
<http://www.juniper.net/techpubs/software/junos/>.

If the information in the latest release notes differs from the information in the documentation, follow the *Junos Release Notes*.

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at  
<http://www.juniper.net/techpubs/>.

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using the Junos operating system (Junos OS) and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security, reliability, and availability using Junos OS configuration techniques. All the books are for sale at technical bookstores and book outlets around the world. The current list can be viewed at <http://www.juniper.net/books>.

## Objectives

---

This guide provides an overview of the mobility features of the Junos OS on the MobileNext Broadband Gateway and describes how to configure these properties on the mobile platform.



**NOTE:** For additional information about Junos OS—either corrections to or information that might have been omitted from this guide—see the software release notes at <http://www.juniper.net/>.

---

---

## Audience

This guide is designed for mobile network administrators who are configuring and monitoring a Juniper Networks MX Series router functioning as a MobileNext Broadband Gateway.

To use this guide, you need a broad understanding of networks in general, the Internet in particular, networking principles, and network configuration. You must also be familiar with one or more of the following Internet routing protocols:

- Border Gateway Protocol (BGP)
- Distance Vector Multicast Routing Protocol (DVMRP)
- Intermediate System-to-Intermediate System (IS-IS)
- Internet Control Message Protocol (ICMP) router discovery
- Internet Group Management Protocol (IGMP)
- Multiprotocol Label Switching (MPLS)
- Open Shortest Path First (OSPF)
- Protocol-Independent Multicast (PIM)
- Resource Reservation Protocol (RSVP)
- Routing Information Protocol (RIP)
- Simple Network Management Protocol (SNMP)

Personnel operating the equipment must be trained and competent; must not conduct themselves in a careless, willfully negligent, or hostile manner; and must abide by the instructions provided by the documentation.

---

## Supported Platforms

For the features described in this manual, the Junos OS currently supports the following platforms:

- MX240 router
- MX480 router
- MX960 router

---

## Documentation Conventions

Table 1 on page xxvii defines notice icons used in this guide.

Table 1: Notice Icons



Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page xxvii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents text that you type.	To enter configuration mode, type the <b>configure</b> command:  <code>user@host&gt; configure</code>
Fixed-width text like this	Represents output that appears on the terminal screen.	<code>user@host&gt; show chassis alarms</code> <code>No alarms currently active</code>
<i>Italic text like this</i>	<ul style="list-style-type: none"> <li>Introduces or emphasizes important new terms.</li> <li>Identifies book names.</li> <li>Identifies RFC and Internet draft titles.</li> </ul>	<ul style="list-style-type: none"> <li>A policy <i>term</i> is a named structure that defines match conditions and actions.</li> <li><i>Junos OS System Basics Configuration Guide</i></li> <li>RFC 1997, <i>BGP Communities Attribute</i></li> </ul>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name:  <code>[edit]</code> <code>root@# set system domain-name <i>domain-name</i></code>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> <li>To configure a stub area, include the <b>stub</b> statement at the <code>[edit protocols ospf area area-id]</code> hierarchy level.</li> <li>The console port is labeled <b>CONSOLE</b>.</li> </ul>
< > (angle brackets)	Enclose optional keywords or variables.	<code>stub &lt;default-metric <i>metric</i>&gt;;</code>

Table 2: Text and Syntax Conventions (*continued*)

Convention	Description	Examples
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	<b>broadcast   multicast</b>  <i>(string1   string2   string3)</i>
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	<b>rsvp { # Required for dynamic MPLS only</b>
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	<b>community name members [ community-ids ]</b>
Indentation and braces ( { } )	Identify a level in the configuration hierarchy.	<b>[edit]</b> <b>routing-options {</b> <b>static {</b> <b>route default {</b> <b>nexthop address;</b> <b>retain;</b> <b>}</b> <b>}</b> <b>}</b>
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
<b>GUI Conventions</b>		
<b>Bold text like this</b>	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> <li>In the Logical Interfaces box, select <b>All Interfaces</b>.</li> <li>To cancel the configuration, click <b>Cancel</b>.</li> </ul>
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select <b>Protocols&gt;Ospf</b> .

## Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net), or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

## Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,

or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

## Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at <http://www.juniper.net/support/requesting-support.html>



## PART 1

# Overview

- [System Architecture on page 3](#)
- [Mobile Network Architecture on page 23](#)
- [Getting Started with Mobile Networks on page 45](#)





## CHAPTER 1

# System Architecture

- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Overview of Broadband Gateway System Control Packet Flow on page 5](#)
- [Overview of Broadband Gateway Uplink Payload Packet Flow on page 7](#)
- [Overview of Broadband Gateway Downlink Payload Packet Flow on page 8](#)
- [Understanding the Broadband Gateway Software Data Path on page 10](#)
- [Overview of Broadband Gateway as GGSN or P-GW on page 11](#)
- [Understanding Mobile User Types on page 12](#)
- [Serving Gateways and the MobileNext Broadband Gateway Overview on page 12](#)
- [Overview of Standalone S-GW User Plane Packet Flow on page 16](#)
- [MobileNext Broadband Gateway Configuration Overview on page 17](#)
- [Overview of Collocated Gateways: Control Plane on page 19](#)
- [Overview of Collocated Gateways: User Plane on page 20](#)

## Overview of Broadband Gateway System Architecture

---

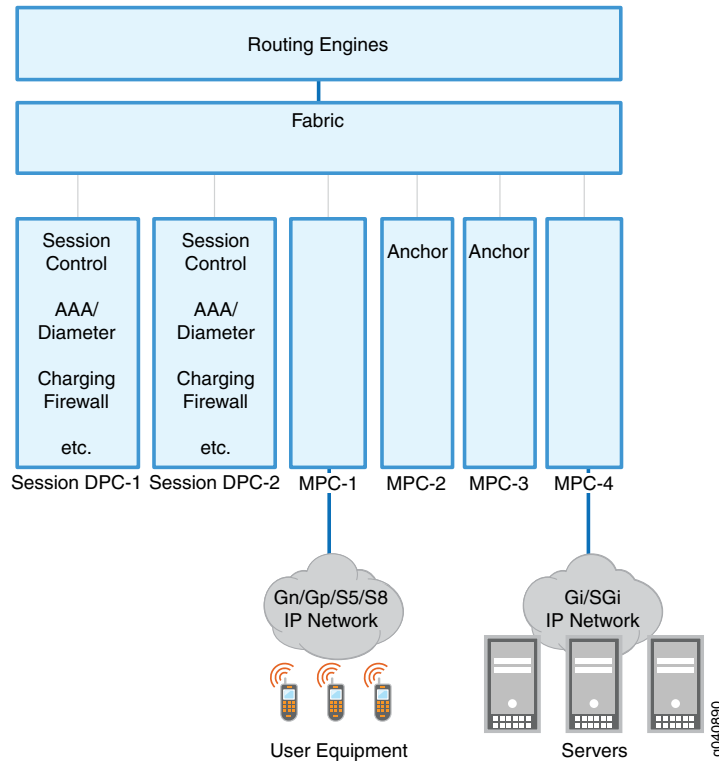
The distinctive architecture of the MobileNext Broadband Gateway allows the functions of the gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW) in 2G, 3G, and 4G architectures to combine with a typical provider edge (PE) router. Service chaining helps with scaling and lets the broadband gateway process mobile traffic without involving the Routing Engine.

[Figure 1 on page 4](#) shows the main hardware components of the broadband gateway. This is a typical configuration: minimally, one session Dense Port Concentrator (DPC) is required and one interface DPC or Modular Port Concentrator (MPC). This configuration shows a more typical configuration for redundancy and other routing functions:

- **Routing Engines**—These components exercise overall control of the chassis.
- **Fabric**—The heart of the chassis, the fabric allows all of the boards to communicate.

- Session DPCs—Also often called Service DPCs, these boards do not have external interfaces, but instead provide services for packets flowing through the system. Some session DPCs are designated *anchor* DPCs for control plane purposes.
- Interface DPCs or MPCs—These boards have external interfaces and can face packet networks or the mobile network. Some of these MPCs are designated anchor MPCs for user (bearer) data flows. All interfaces can use a single IP address.

**Figure 1: The Broadband Gateway System Architecture**



An *anchor* session DPC is where mobile control plane functions occur for a particular subscriber. The anchor interface DPC or MPC is where the processing for a specific GPRS tunneling protocol (GTP) tunnel identifier range occurs.

A key feature of the broadband gateway architecture is that many services can be integrated into the system. It is important to note that these services can be performed in a single pass through the device. This simplifies deployment scenarios and reduces requirements for space, latency, power, cooling, and so on. Because everything is all in one system, there are no interoperability issues and the same network management system can be used.

The broadband gateway can support 2G, 3G, and 4G subscribers at the same time, features fully redundant hardware and resilient software, and can scale bearer and control planes separately.

An overall resource manager watches operations concerning the resource management clients (the board in the chassis slots) and server (the active Routing Engine) on the broadband gateway.



**NOTE:** You do not configure the resource manager for the broadband gateway. The process runs automatically.

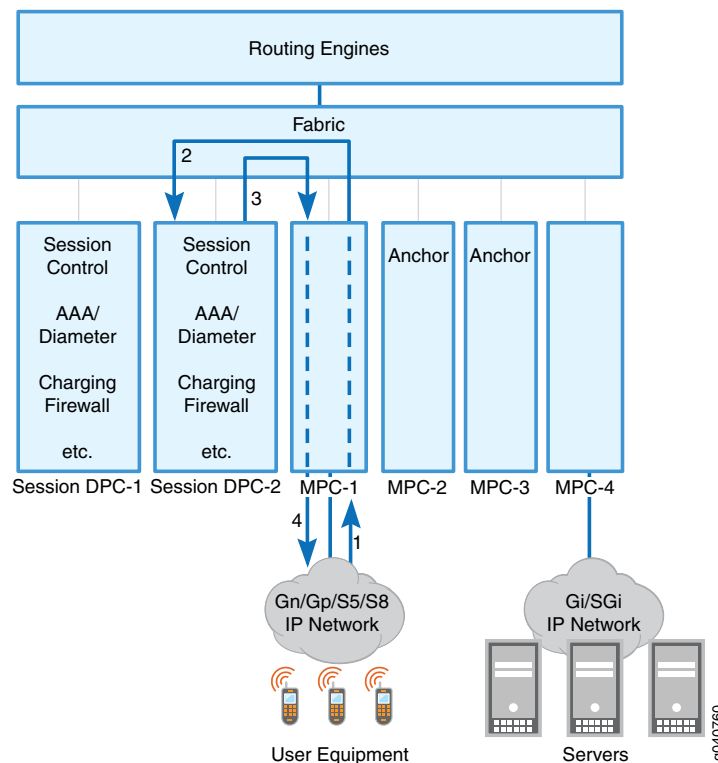
**Related Documentation**

- [Overview of Broadband Gateway System Control Packet Flow on page 5](#)
- [Overview of Broadband Gateway Uplink Payload Packet Flow on page 7](#)
- [Overview of Broadband Gateway Downlink Payload Packet Flow on page 8](#)
- [Overview of Broadband Gateway as GGSN or P-GW on page 11](#)

## Overview of Broadband Gateway System Control Packet Flow

The MobileNext Broadband Gateway uses session Dense Port Concentrators (DPCs) to handle all GPRS tunneling protocol, control (GTP-C) signaling requests from the user equipment and the GTP responses. New GTP sessions are anchored on a selected session DPC, and all control plane functions are handled by the same session DPC. In this example, the mobile and packet network interfaces are all housed in Modular Port Concentrators (MPCs).

**Figure 2: Broadband Gateway GTP Signaling Packet Flow**



[Figure 2 on page 5](#) shows the four steps that GTP-C signaling packets take through the broadband gateway:

1. An attached user equipment device activates a session and sends a Create Session request GTP-C signaling packet to a mobile interface on the broadband gateway.
2. The Gn/Gp or S5/S8 interface MPC parses the GTP-C packet based on the outer IP address and selects a session DPC for the new session. The MPC then sends the GTP-C signaling packet through the fabric to a session DPC that will anchor the session for control purposes. The session DPC performs the admission control, authentication, authorization, and accounting (AAA), Dynamic Host Configuration Protocol (DHCP) and charging operations required.
3. If the session is accepted, the session DPC sends a create session reply GTP-C signaling packet to the interface MPC that received the GTP message.
4. The Gn/Gp or S5/S8 interface MPC sends the GTP-C response back to the user equipment.

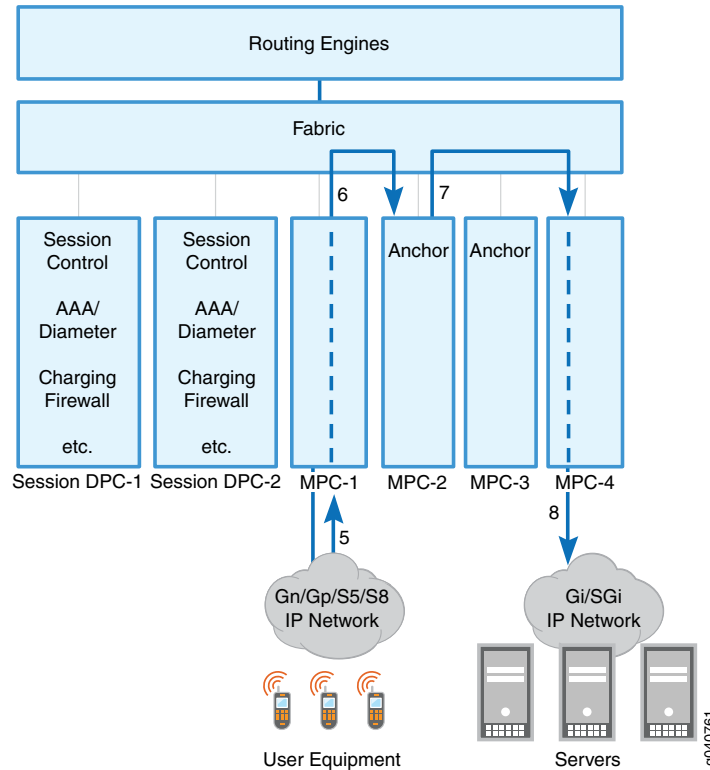
**Related  
Documentation**

- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Overview of Broadband Gateway Uplink Payload Packet Flow on page 7](#)
- [Overview of Broadband Gateway Downlink Payload Packet Flow on page 8](#)
- [Overview of Broadband Gateway as GGSN or P-GW on page 11](#)

## Overview of Broadband Gateway Uplink Payload Packet Flow

The MobileNext Broadband Gateway uses interface Modular Port Concentrators (MPCs) or Dense Port Concentrators (DPCs) to handle all uplink user payload packet flow requests from user equipment. All user traffic flows through the anchor interface MPC or DPC. In this example, the mobile and packet network interfaces are all housed in MPCs.

**Figure 3: Broadband Gateway Uplink User Packet Flow**



After the GPRS tunneling protocol control (GTP-C) packets establish a session, [Figure 3 on page 7](#) shows the next four steps that the uplink user payload GTP user plane (GTP-U) packets take through the broadband gateway:

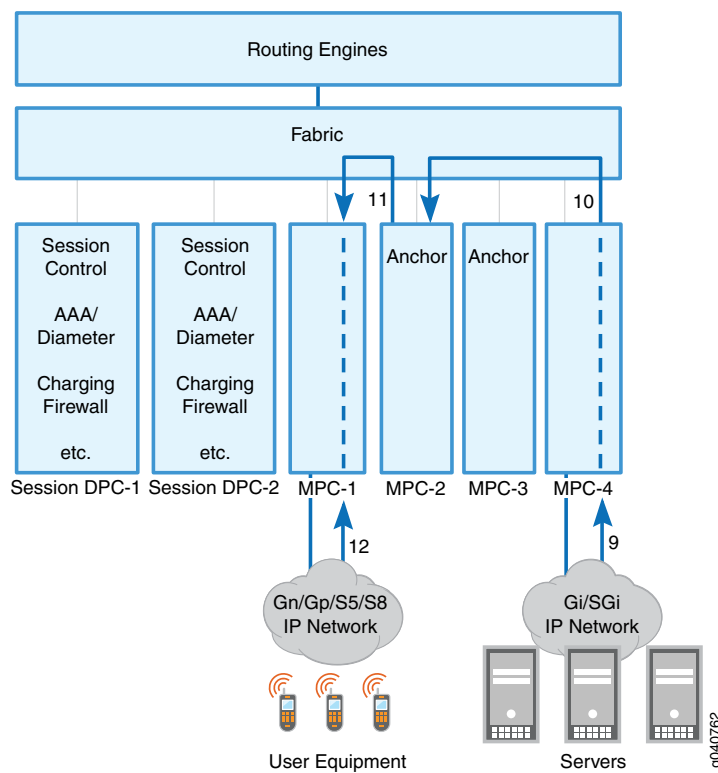
5. An attached user equipment device sends an uplink payload GTP-U packet to a mobile interface on the broadband gateway.
6. The interface MPC sends the GTP-U packet to the interface MPC chosen during the control phase to anchor the user session data flow. The anchor MPC performs all subscriber-specific access control, policing, statistic gathering, and other parameters set for the subscriber based on the inner IP address in the GTP-U packet.
7. The anchor interface MPC sends the user packet to the uplink MPC that leads to the correct IP packet network.
8. The uplink interface MPC sends the user payload packet to the IP network on the Gi or SGi interface.

- Related Documentation**
- [Overview of Broadband Gateway System Architecture on page 3](#)
  - [Overview of Broadband Gateway System Control Packet Flow on page 5](#)
  - [Overview of Broadband Gateway Downlink Payload Packet Flow on page 8](#)
  - [Overview of Broadband Gateway as GGSN or P-GW on page 11](#)

## Overview of Broadband Gateway Downlink Payload Packet Flow

The MobileNext Broadband Gateway uses interface Modular Port Concentrators (MPCs) or Dense Port Concentrators (DPCs) to handle all downlink user payload packets flows requests from an IP network back to the user equipment. All user traffic flows through the anchor interface MPC or DPC. In this example, the mobile and packet network interfaces are all housed in MPCs.

**Figure 4: Broadband Gateway Downlink User Packet Flow**



After the GPRS tunneling protocol, control (GTP-C) packets establish a session, and packets flow uplink to the broadband gateway, [Figure 4 on page 8](#) shows the last four steps that the downlink user payload GTP user plane (GTP-U) packets take through the broadband gateway:

9. The IP network sends a downlink data packet to a mobile Gi or SGi interface on the broadband gateway.
10. The interface MPC sends the downlink packet to the interface MPC chosen during the control phase to anchor the user session data flow. The anchor MPC performs all subscriber-specific access control, policing, statistic gathering, and other parameters set for the subscriber.
11. The anchor interface MPC sends the encapsulated GTP-U packet to the downlink interface that leads to the correct user device.
12. The downlink interface MPC sends the GTP-U user payload packet to the user device.

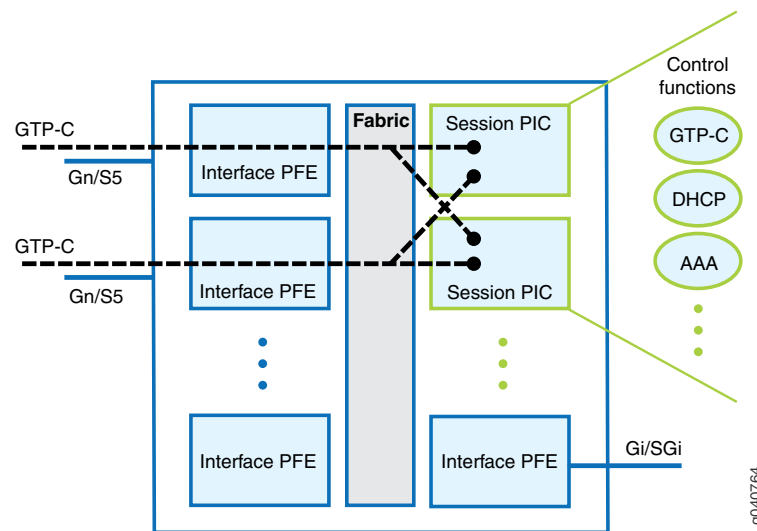
**Related  
Documentation**

- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Overview of Broadband Gateway System Control Packet Flow on page 5](#)
- [Overview of Broadband Gateway Uplink Payload Packet Flow on page 7](#)
- [Overview of Broadband Gateway as GGSN or P-GW on page 11](#)

## Understanding the Broadband Gateway Software Data Path

The MobileNext Broadband Gateway processes GPRS tunneling protocol (GTP) and IP packets as they make their way from an input interface to an output interface, upstream from mobile device to IP network or downstream from IP network to mobile device. Usually, the packet processing is handled at the “hardware” level, in the interface and anchor Packet Forwarding Engines. However, certain *data path* (sometimes called “exception”) packets follow a path through “software”, which means the Session PIC.

### Figure 5: GTP-C Handling



As shown in [Figure 5 on page 10](#), control plane packets such as session creation requests arriving on a Gn or S5 (or S8) interface are sent to an anchor session Dense Port Concentrator (DPC) for processing. The session DPC load-balances and selects anchor interface DPCs or Modular Port Concentrators (MPCs) (housing the Packet Forwarding Engines) for the user session, and all subsequent data packets for that session flow through the anchor Packet Forwarding Engine. Mid-session control packets, such as those changing session parameters due to mobility, are still sent to the anchor session DPC and associated PICs. In general, upstream and downstream data flows are handled directly by the anchor Packet Forwarding Engine.

There are four exceptions to the general rule that user packets flow only through Packet Forwarding Engine hardware:

- Anchor Packet Forwarding Engine failovers (N:1)
- Reassembly of GTP-U and mobility control plane (for instance, authentication, authorization, and accounting [AAA]) fragments
- IPv6 router advertisements and router solicitation packet handling
- GTP-U error indication generation



Only software-based IP fragment reassembly and IPv6 router advertisements have parameters you can configure on the broadband gateway. (Anchor Packet Forwarding Engine configuration is part of the basic chassis configuration and aggregated Packet Forwarding Engines for failover are part of redundancy configuration).

**Related  
Documentation**

- [Understanding GTP-U Error Data Path on page 300](#)
- [Configuring GGSN or P-GW Software Data Path Traceoptions on page 55](#)
- [Configuring S-GW Software Data Path Traceoptions on page 62](#)

## Overview of Broadband Gateway as GGSN or P-GW

You can configure the MobileNext Broadband Gateway as either a 3G gateway GPRS support node (GGSN) or 4G Packet Data Network Gateway (P-GW). The GGSN or P-GW is the interconnection point between the public land mobile network (PLMN) and a particular Packet Data Network (PDN) such as the Internet or a corporate intranet.

In 3G networks, the GGSN maintains a one-to-many relationship with serving GPRS support nodes (SGSNs), which may be in either the home public land mobile network (HPLMN) or visited public land mobile network (VPLMN) for roaming subscribers. The SGSN and GGSN communicate with each other over Gn interface, which utilizes GPRS tunneling protocol, control plane (GTP-C) (version 0 and version 1) and GPRS tunneling protocol, user plane (GTP-U) for data traffic.

In 4G networks, the P-GW maintains a one-to-many relationship with Serving Gateway (S-GW), which can be in either the home PLMN or visiting PLMN for roaming subscribers. The S-GW and P-GW communicate with each other over the S5 interface for non-roaming subscribers and S8 interface for roaming subscribers. Both S5 and S8 interfaces make use of GTP-C (version 2) for control plane and GTP-U for data traffic.

The application framework for the broadband gateway is composed of a set of applications and protocols that interact with the external servers and provide the following configurable services for subscribers:

- Mobile subscriber authentication with RADIUS.
- Charging and accounting with GTP prime Charging Data Records (CDRs) generation and billing, or through RADIUS accounting.
- Policy enforcement using local configuration.

You configure the GGSN or P-GW for the broadband gateway as part of a *unified edge* configuration. The unified edge brings all mobile subscriber-related services under one structure. A unified edge gateway has its own set of parameters for AAA, charging, APNs, and so on.

**Related  
Documentation**

- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Configuring Broadband Gateway Home PLMNs and Gateways on page 45](#)

## Understanding Mobile User Types

---

There are different types of users in a mobile network. These are distinguished by comparing the home public land mobile network (HPLMN) list configured on the gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW) and the PLMNs received from users in headers and control messages.

Based on a comparison of PLMNs, the mobile user falls into one of three categories:

- Home user—The subscriber, the GGSN or P-GW, and SSGN or S-GW are all in the same PLMN.
- Roaming user—The subscriber and GGSN or P-GW belong to the same PLMN, but the SSGN or S-GW are in a different PLMN.
- Visiting user—The subscriber and SGSN or S-GW belong to the same PLMN, but the GGSN or P-GW are in a different PLMN.

### Related Documentation

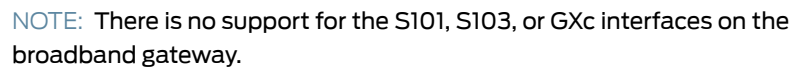
- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Configuring Broadband Gateway Home PLMNs and Gateways on page 45](#)
- [Configuring Broadband Gateway Local Policies Application on page 46](#)

## Serving Gateways and the MobileNext Broadband Gateway Overview

---

In a 4G mobile network, the MobileNext Broadband Gateway can function as a standalone Serving Gateway (S-GW), or collocate the S-GW on the same broadband gateway as a Packet Data Network Gateway (P-GW). Note that the collocated S-GW feature is only available on 4G configurations. You cannot configure the broadband gateway as a Serving GPRS Support Node (SGSN) as part of a General GPRS Support Node (GGSN).

The S-GW includes features that facilitate connection to the radio or mobile device side of the mobile network. Many of these functions involve maintaining the end-to-end connectivity between user equipment on the Radio Access Network (RAN) and gateway to IP-based services in the Packet Data Network (PDN) in an environment where users are constantly moving around. The key S-GW interfaces are shown in [Figure 6 on page 13](#).



The fundamental interface of the S-GW is the S1 interface. The X2 interface is related, but X2 is not configured on the S-GW because the X2 interface connects one eNodeB to another. The S1 interface connects an eNodeB to Evolved Packet Core (EPC), in particular, the S-GW. Both the X2 and S1 interfaces are IP-based and include separate user plane and control plane protocol stacks. Application protocols define the signalling messages and procedures sent across the X2 and S1 interfaces.

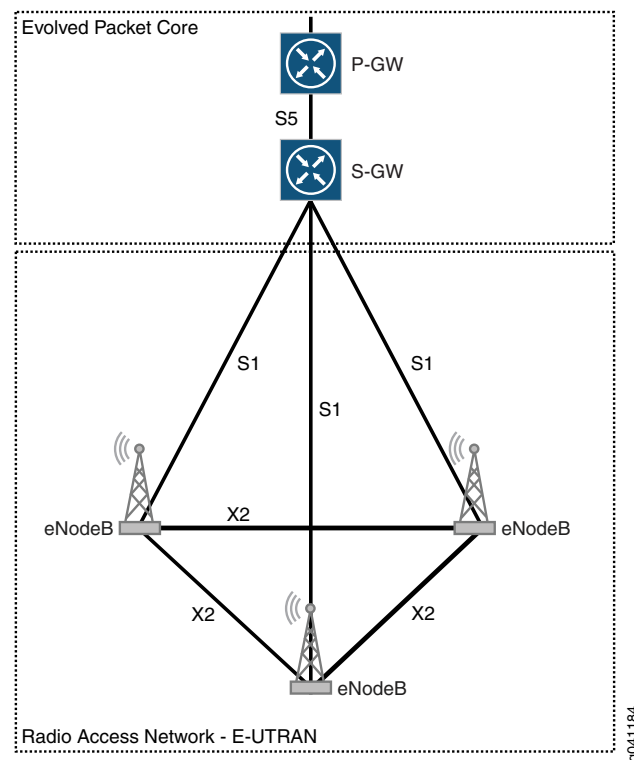
The S1 control plane runs between an eNodeB and a Mobility Management Entity (MME) and is called the S1-MME. Do not confuse the S1-MME (eNodeB-MME interface) with the S11 (S-GW-MME) interface, which carries GPRS tunneling protocol control (GTP-C) messages. On the other hand, the S1 user plane runs between the eNodeB and the S-GW and is called the S1-U interface and carries GTP user (GTP-U) payloads.

When the broadband gateway is configured as an S-GW, the S-GW provides the following hand-over capabilities:

- S1 interface (eNodeB to MME) hand-over with S-GW relocation
- S1 interface (eNodeB to MME) hand-over *without* S-GW relocation
- End marker packet support to downlink eNodeB when a path switch is made from the old eNodeB
- Indirect forwarding tunnels when there is no user plane available between source eNodeB and target eNodeB (or RNC)
- X2 interface (eNodeB to eNodeB) hand-over with S-GW relocation
- X2 interface (eNodeB to eNodeB) hand-over *without* S-GW relocation

[Figure 7 on page 15](#) shows the relationship between the S1 and X2 interfaces.

Figure 7: S-GW and the S1 and X2 Interfaces



#### Related Documentation

- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Overview of Standalone S-GW User Plane Packet Flow on page 16](#)
- [Overview of Collocated Gateways: Control Plane on page 19](#)
- [Overview of Collocated Gateways: User Plane on page 20](#)
- [MobileNext Broadband Gateway Configuration Overview on page 17](#)
- [Configuring an S-GW on a Broadband Gateway on page 57](#)
- [Configuring S-GW-Specific Profiles on page 58](#)
- [Configuring S-GW Traceoptions on page 59](#)

## Overview of Standalone S-GW User Plane Packet Flow

The architecture of the MobileNext Broadband Gateway, when configured as a Serving Gateway (S-GW) allows GPRS tunneling protocol (GTP) packets to pass efficiently from input to output interface.

**Figure 8: GTP-U Packet Flow Through Standalone S-GW**

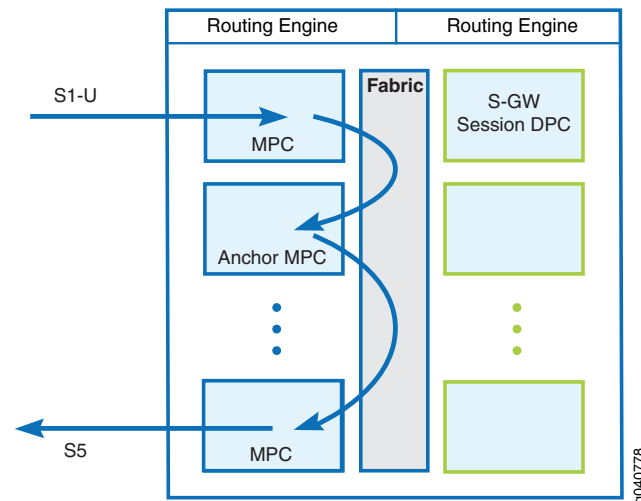


Figure 8 on page 16 shows the usual path of user packets (GTP-U) from eNodeB radio network (S1-U) to P-GW (S5) interfaces. Note that the user packet passes through the S-GW anchor Modular Port Concentrator (MPC) for that particular bearer. They do not flow through a service Packet Forwarding Engine unless absolutely necessary.

For user packet flows, the anchor MPC provides:

- Line rate GTP packet processing
- Stitching together of packet streams and packet forwarding
- Extremely low latency
- Hardware-based quality of service (QoS)
- Traffic counters and charging information

When necessary, the services Packet Forwarding Engine provides the following for the user packet flow:

- IP Security (IPsec)
- Internet Key Exchange (IKE)



**NOTE:** The broadband gateway can have other services Packet Forwarding Engines that are not associated with the S-GW.

**Related Documentation**

- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Serving Gateways and the MobileNext Broadband Gateway Overview on page 12](#)
- [Overview of Collocated Gateways: Control Plane on page 19](#)
- [Overview of Collocated Gateways: User Plane on page 20](#)
- [MobileNext Broadband Gateway Configuration Overview on page 17](#)
- [Configuring an S-GW on a Broadband Gateway on page 57](#)
- [Configuring S-GW-Specific Profiles on page 58](#)
- [Configuring S-GW Traceoptions on page 59](#)

## MobileNext Broadband Gateway Configuration Overview

The MobileNext Broadband Gateway offers flexible configuration to best service mobile subscribers. Different users can utilize the same broadband gateway chassis as a Packet Data Network Gateway (P-GW), a Service Gateway (S-GW), or both.

**Figure 9: Collocated Gateways S-GW and P-GW Resources and Load Balancing**

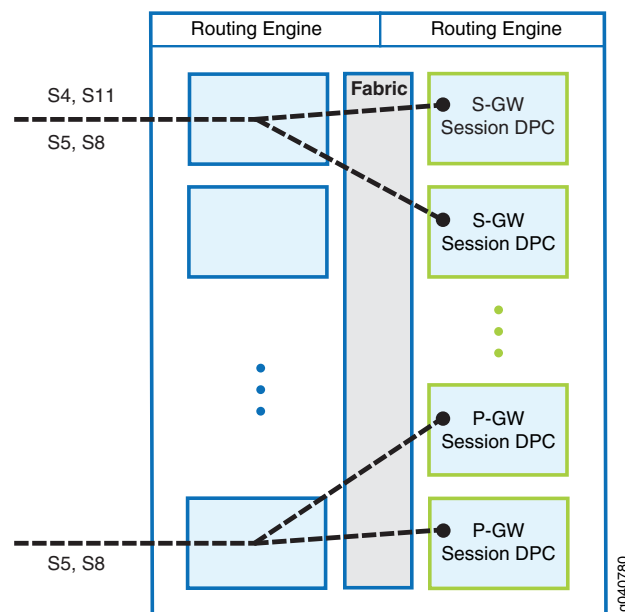


Figure 9 on page 17 shows how resource sharing and load balancing takes place in a collocated S-GW and P-GW configured on the broadband gateway. No matter how the broadband gateway is utilized, the chassis configuration for Modular Port Concentrators (MPCs), Dense Port Concentrators (DPCs), anchors, and session and services DPCs is the same. This topic concerns functional configuration of the installed and configured hardware.

The session DPCs are dedicated (and load balanced) for P-GW and S-GW functions. Resources are not shared between S-GW and P-GW session DPCs. The resources of each DPC are dedicated to either one function or the other.



**NOTE:** You can only configure a session DPC to support the S-GW or the P-GW function. A DPC cannot be configured as part of both at the same time. If you try to configure the chassis this way, the commit operation will fail.

You can configure the broadband gateway so that separate mobile subscribers see the gateway as one of the following:

- P-GW
- S-GW
- Collocated P-GW and S-GW



**NOTE:** You can also configure multiple collocated P-GWs and S-GWs on the same chassis.

You assign various mobile subscribers to their respective gateways, packet networks, and mobile services.

**Related  
Documentation**

- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Serving Gateways and the MobileNext Broadband Gateway Overview on page 12](#)
- [Overview of Collocated Gateways: Control Plane on page 19](#)
- [Overview of Collocated Gateways: User Plane on page 20](#)
- [Configuring an S-GW on a Broadband Gateway on page 57](#)
- [Configuring S-GW-Specific Profiles on page 58](#)
- [Configuring S-GW Traceoptions on page 59](#)



## Overview of Collocated Gateways: Control Plane

You can configure the MobileNext Broadband Gateway as a collocated Serving Gateway (S-GW) and Packet Data Network Gateway (P-GW). GPRS Tunneling Protocol, control (GTP-C) packets pass through their respective session Dense Port Concentrators (DPCs).

**Figure 10: Collocated S-GW and P-GW Control Packet Flow**

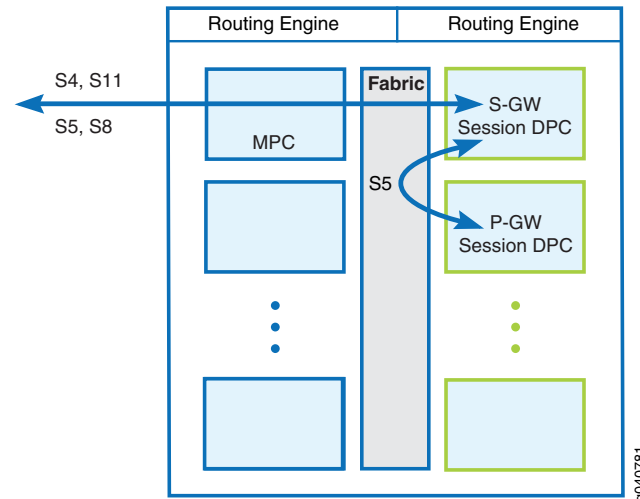


Figure 10 on page 19 shows the path of GTP-C packets through the broadband gateway when configured as a collocated S-GW and P-GW.

The Routing Engine(s) provide:

- Chassis management
- Storage of Charging Data Records (CDRs)
- A point for operations and management

The interface Modular Port Concentrators (MPCs) provide load balancing of the control plane packets and form a single network element.

The session DPCs constitute the mobility control plane and provide seamless 2G, 3G, or 4G subscriber management and multiple functions on the same card.

The control plane also handles all control functions such as GTP-C processing, charging using GTP-prime, Dynamic Host Configuration Protocol (DHCP) functions, and Authentication, Authorization, and Accounting (AAA) functions.

### Related Documentation

- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Serving Gateways and the MobileNext Broadband Gateway Overview on page 12](#)
- [Overview of Standalone S-GW User Plane Packet Flow on page 16](#)
- [Overview of Collocated Gateways: User Plane on page 20](#)

- [Configuring an S-GW on a Broadband Gateway on page 57](#)
- [Configuring S-GW-Specific Profiles on page 58](#)
- [Configuring S-GW Traceoptions on page 59](#)

## Overview of Collocated Gateways: User Plane

You can configure the MobileNext Broadband Gateway as a collocated Serving Gateway (S-GW) and Packet Data Network Gateway (P-GW). All GPRS tunneling protocol (GTP) packets pass efficiently from input to output interface through their respective anchor Modular Port Concentrators (MPCs).

**Figure 11: Collocated S-GW and P-GW User Packet Flow**

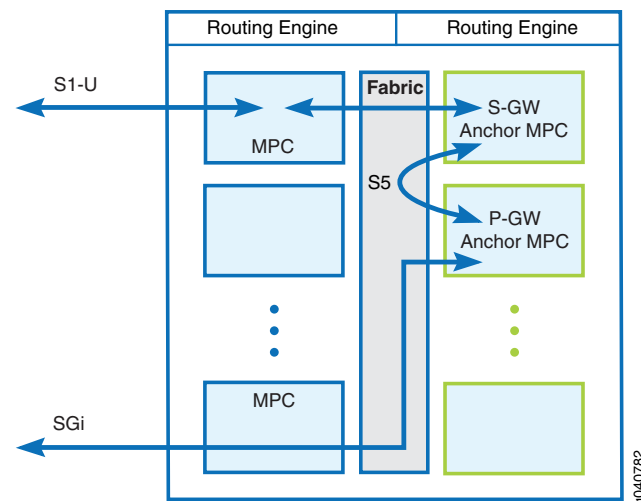


Figure 11 on page 20 shows a collocated P-GW and S-GW in the same broadband gateway. The usual path of user packets from eNodeB radio network (S1-U) to internal S5 interface to SGi interface is shown. Note that the user packet passes through the S-GW and P-GW anchor Modular Port Concentrators (MPCs) for a particular bearer, but the packets do not flow through a services Packet Forwarding Engine unless absolutely necessary.

For user packet flows, the anchor MPC provides:

- Line rate GTP packet processing
- Stitching together of packet streams and packet forwarding
- Extremely low latency
- Hardware-based quality of service (QoS)
- Traffic counters and charging information

When necessary, the services Packet Forwarding Engine provides the following for the user packet flow:

- IP Security (IPsec)
- Internet Key Exchange version 2 (IKEv2)
- Network Address Translation (NAT) and forwarding
- Deep Packet Inspection (DPI)



**NOTE:** The broadband gateway can have other services PFEs that are not associated with the S-GW or P-GW.

---

**Related  
Documentation**

- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Serving Gateways and the MobileNext Broadband Gateway Overview on page 12](#)
- [Overview of Standalone S-GW User Plane Packet Flow on page 16](#)
- [Overview of Collocated Gateways: Control Plane on page 19](#)
- [Configuring an S-GW on a Broadband Gateway on page 57](#)
- [Configuring S-GW-Specific Profiles on page 58](#)
- [Configuring S-GW Traceoptions on page 59](#)



## CHAPTER 2

# Mobile Network Architecture

- [Overview of Mobile Networks on page 23](#)
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 25](#)
- [Overview of GGSN and P-GW on page 26](#)
- [Overview of Packet Data Network Gateway Functions on page 28](#)
- [Overview of the Evolved Packet Core on page 30](#)
- [Overview of APNs on page 32](#)
- [Overview of PDP Contexts and Bearers on page 33](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 35](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 36](#)
- [Overview of IPv6 and the Broadband Gateway on page 38](#)
- [Serving Gateway and the S1 Interface Overview on page 39](#)
- [Service Areas and Tracking Areas Overview on page 40](#)
- [Serving Gateway Functions Overview on page 41](#)

## Overview of Mobile Networks

---

Mobile (cellular) networks have evolved rapidly as analog voice gave way to digital voice, and now routinely include data services and streaming digital video, all delivered to the mobile device or user equipment over an IP network. Although not directly part of 4G or the Long Term Evolution (LTE) of mobile networks, some background on the 3G mobile architecture and the 3G packet gateway, or gateway GPRS support node (GGSN), is necessary. This is because the Packet Data Network Gateway (P-GW) in the LTE architecture is still expected to internetwork and interoperate with 3G (and often even older) architectures and devices.

The major generations of mobile network architectures are:

- “1G”—The first generation; of course, no one called this type of mobile network “1G” because no one knew there would be subsequent generations. It supported analog voice bandwidths and did not support GPRS data.
- 2G—Once mobile networks proved popular, the next step digitized the radio signal (which added capacity and was spectrally more efficient) and added some rudimentary data capabilities through the Global System for Mobile Communications (GSM)

standard. Phone conversations were now digitally encrypted and text messaging (short message service, or SMS) began, although it would take years before most devices supported such messages. Enhanced mobile networks added digital services such as GPRS or Enhanced Data Rates for GSM Evolution (EDGE). Many mobile networks are still some form of 2G networks. The gateway GPRS support node (GGSN) was included in these advanced architectures.

- 3G—The many flavors of 2G networks led to the formation of the 3G Partnership Project (3GPP) to standardize the next generation of mobile networks. The universal mobile telecommunications system (UMTS) was standardized by the 3GPP and is widely used around the world. Today, many cell phones are GSM/UMTS hybrids. The latest UMTS release is called High Speed Packet Access (HSPA and HSPA+), offering higher bit rates.
- 4G and LTE—The fourth generation of mobile networks is defined by the International Telecommunication Union (ITU) as 4G. The 3GPP has also created a standard to provide a context for the “long-term evolution” of mobile networks (LTE) and LTE Advanced.

As time goes by, the designations 3G and 4G have become more marketing terms than architectural standards.

**Related  
Documentation**

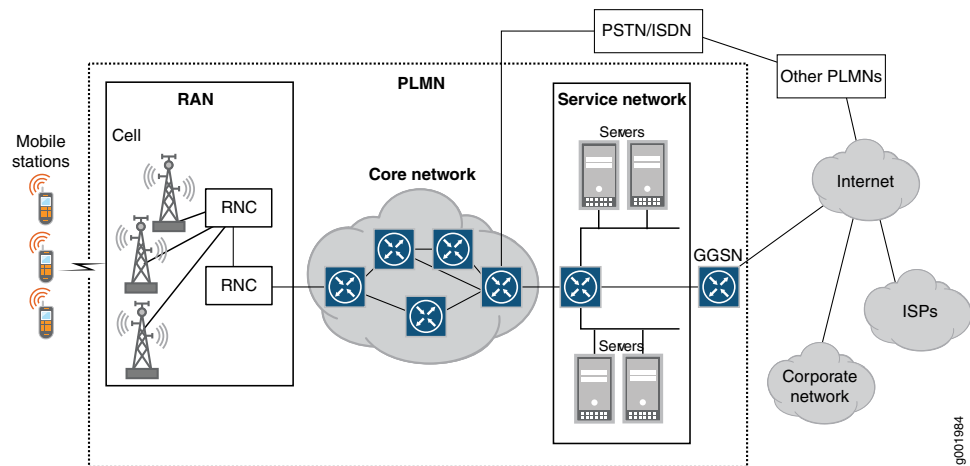
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 25](#)
- [Overview of GGSN and P-GW on page 26](#)
- [Overview of Packet Data Network Gateway Functions on page 28](#)
- [Overview of the Evolved Packet Core on page 30](#)
- [Overview of APNs on page 32](#)
- [Overview of PDP Contexts and Bearers on page 33](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 35](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 36](#)
- [Overview of IPv6 and the Broadband Gateway on page 38](#)
- [Overview of IPv6 and the Broadband Gateway on page 38](#)
- [Serving Gateway and the S1 Interface Overview on page 39](#)
- [Serving Gateway and the S1 Interface Overview on page 39](#)
- [Service Areas and Tracking Areas Overview on page 40](#)

## Overview of 3G Mobile Networks and the MobileNext Broadband Gateway

Third generation (3G) mobile networks define three components of the overall path from mobile station to IP network: the radio frequencies used, the air interface options used between the mobile device and base station, and the entire network architecture, including interfaces between components.

Figure 12 on page 25 shows the overall architecture of a 3G network. The MobileNext Broadband Gateway is configured as the gateway GPRS support node (GGSN) in this architecture.

Figure 12: 3G Mobile Network Architecture



**NOTE:** The GGSN is not properly part of the 3G “service network.”

There are three major parts to a 3G mobile network:

- A Radio Access Network (RAN). This is a hierarchical arrangement of cell towers and base stations. The base stations are called base transceiver stations (BTs) or NodeBs in 3G. In some versions, there are also Radio Network Controllers (RNCs) that link to the BTs to form a Radio Network Subsystem (RNS). A collection of RNSs using the Wideband CDMA (WCDMA) air interface option form the UMTS Terrestrial Radio Access Network (UTRAN). All of these are referred to as “network devices” in Figure 12 on page 25. The important point is that all handovers between cell towers are centrally controlled in the 3G network hierarchy.
- A core network (usually IP) tying the RAN to the 3G service network. The core network consists of all the switches, routers, and other network components required to transport mobile traffic.
- A service network reached through the core network. Some of the services reached (the servers in Figure 12 on page 25) are specific to the service provider, such as accounting information (current balance), short message service (SMS) texting, paging, and voice mail. Other services are reached through the GGSN (which is not properly

part of the 3G service network), such as the Internet, other Internet service providers (ISPs), or corporate network virtual private networks (VPNs). The MobileNext Broadband Gateway can be configured as a GGSN.

Together in 3G, the RAN, core network, and service network (and GGSN) make up the public land mobile network (PLMN). A PLMN ("land" network) is distinguished from a marine network.

**Related  
Documentation**

- [Overview of Mobile Networks on page 23](#)
- [Overview of GGSN and P-GW on page 26](#)
- [Overview of Packet Data Network Gateway Functions on page 28](#)
- [Overview of the Evolved Packet Core on page 30](#)
- [Overview of APNs on page 32](#)
- [Overview of PDP Contexts and Bearers on page 33](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 35](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 36](#)
- [Overview of IPv6 and the Broadband Gateway on page 38](#)
- [Overview of IPv6 and the Broadband Gateway on page 38](#)
- [Serving Gateway and the S1 Interface Overview on page 39](#)
- [Serving Gateway and the S1 Interface Overview on page 39](#)
- [Service Areas and Tracking Areas Overview on page 40](#)

---

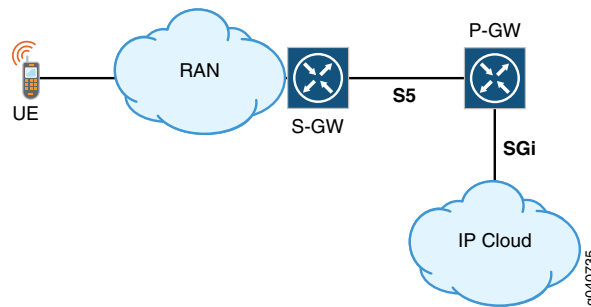
## Overview of GGSN and P-GW

The Juniper Networks MobileNext Broadband Gateway can act as a gateway GPRS support node (GGSN) in a 2G and 3G network architecture, a Packet Data Network Gateway (P-GW) in a 4G/LTE network architecture, or even both at the same time. When it comes to user traffic, the differences are mainly in the terms used to refer to the "mobile-facing" side of the gateway and not the IP data side.

[Figure 13 on page 27](#) shows the major components and interfaces of a mobile network based on 4G/LTE standards.



Figure 13: 4G/LTE Mobile Network Basic Components



The major components are:

- User equipment (UE)—Often called the “mobile platform” in other standards. The user equipment can be a mobile smartphone, a “dongle” used to enable service on another device, a laptop, or even other compliant devices.
- RAN (Radio Access Network)—The RAN is called the universal terrestrial radio access network (UTRAN) in the 3G Universal Mobile Telecommunications System (UMTS) architecture (sometimes UTRAN is defined as UMTS Terrestrial Radio Access Network). In the LTE architecture, the RAN is the evolved UTRAN, or E-UTRAN.
- S-GW—In the LTE architecture, the node that handles all signaling messages to and from the user equipment is called the Serving Gateway (S-GW). (The SGSN in 3G networks is different from the S-GW in 4G networks.).
- P-GW—In 2G and 3G networks, the node that handled all user packets to and from the user equipment is called the GGSN. In the LTE architecture, this is the Packet Gateway (P-GW) or sometimes seen as the Packet Data Network Gateway (PDN-GW).
- IP Cloud— This is the Packet Data Network (PDN) in 2G and 3G and LTE. However, LTE adds another type of IP network, called IP Multimedia Services (IMS). IMS networks essentially handle VoIP calls to and from the user equipment.

From the GGSN/P-GW perspective, the major interfaces in the figure are:

- S5—In 4G/LTE, the S5 interface connects the P-GW to the mobile side of the network (for home users). In 3G, this is the Gn (“n” for network) interface.
- Gi/SGi—In 4G/LTE, the SGi interface connects the P-GW to the IP packet side of the network. In 3G, this is the Gi (“i” for Internet or IP network) interface.

#### Related Documentation

- [Overview of Mobile Networks on page 23](#)
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 25](#)
- [Overview of Packet Data Network Gateway Functions on page 28](#)
- [Overview of the Evolved Packet Core on page 30](#)
- [Overview of APNs on page 32](#)
- [Overview of PDP Contexts and Bearers on page 33](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 35](#)

- [Overview of 4G/LTE and Broadband Gateway Deployment on page 36](#)
- [Overview of IPv6 and the Broadband Gateway on page 38](#)
- [Overview of IPv6 and the Broadband Gateway on page 38](#)
- [Serving Gateway and the S1 Interface Overview on page 39](#)
- [Serving Gateway and the S1 Interface Overview on page 39](#)
- [Service Areas and Tracking Areas Overview on page 40](#)

## Overview of Packet Data Network Gateway Functions

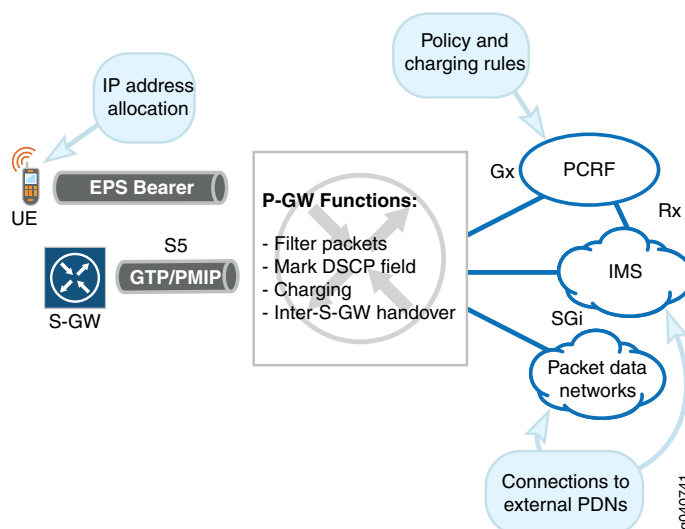
In a mobile network, a major function of the Packet Data Network Gateway (P-GW) is to allocate IP addresses to the user equipment during default bearer setup. The user equipment can still connect to multiple packet networks through multiple P-GWs, and also to older, non-3GPP-compliant IP networks.



**NOTE:** The MobileNext Broadband Gateway does not support interfaces to non-3GPP IP networks.

In the Long Term Evolution (LTE) architecture for the Evolved Packet Core (EPC), the P-GW acts as an anchor for user plane mobility. User traffic can be filtered at the P-GW for quality-of-service (QoS) differentiation among multiple packet flows. The P-GW collects charging information and forwards these Charging Data Records (CDRs) for processing.

**Figure 14: Packet Data Network Gateway Functions**





**NOTE:** The MobileNext Broadband Gateway does not initially support inter-S-GW handovers, connectivity to Non-3GPP IP networks, or direct rate enforcement.

The important interfaces on the P-GW shown in [Figure 14 on page 28](#) are:

- **EPS Bearer**—This is the interface to the user equipment associated with the P-GW. It is a tunnel and used for IP address allocation and other purposes.
- **Rx**—Although not a direct P-GW interface, this interface is used for all kinds of unsolicited reporting between the policy and charging rules function (PCRF) and the IP Multimedia Subsystem (IMS) network. The IMS delivers services such as voice over IP (VoIP) to the user equipment. This interface uses the Diameter protocol over Stream Control Transport Protocol (SCTP) and TCP, and passes the PCRF permissions to the service network.
- **SGi**—This is the interface to the IMS and other internal and external Packet Data Networks (PDNs), where services are usually rendered. Examples are IMS for voice, Web portals, simple Internet access, and so on. All traffic is in the form of IP packets and flows.
- **S5**—This is the interface to the Serving Gateway (S-GW) associated with the P-GW. This interface supports the GPRS tunneling protocol (GTP) for the user plane.

#### Related Documentation

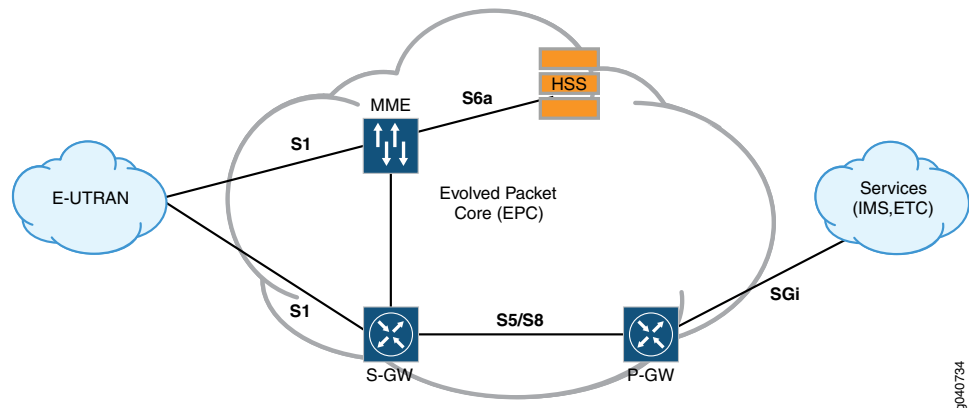
- [Overview of Mobile Networks on page 23](#)
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 25](#)
- [Overview of GGSN and P-GW on page 26](#)
- [Overview of the Evolved Packet Core on page 30](#)
- [Overview of APNs on page 32](#)
- [Overview of PDP Contexts and Bearers on page 33](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 35](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 36](#)
- [Overview of IPv6 and the Broadband Gateway on page 38](#)
- [Overview of IPv6 and the Broadband Gateway on page 38](#)
- [Serving Gateway and the S1 Interface Overview on page 39](#)
- [Serving Gateway and the S1 Interface Overview on page 39](#)
- [Service Areas and Tracking Areas Overview on page 40](#)

## Overview of the Evolved Packet Core

The Juniper Networks MobileNext Broadband Gateway, as a Packet Data Network Gateway (P-GW), is a key component of the Long Term Evolution (LTE) architecture's Evolved Packet Core (EPC). The P-GW faces the IP service and networks, and the Serving Gateway (S-GW) faces the radio network. Together, they provide the user plane from the IP packet network to the Radio Access Network (RAN). However, a few other EPC devices are necessary as well.

Figure 15 on page 30 shows the major components and interfaces of the EPC of a mobile network based on LTE standards. The user equipment can attach to only one Mobility Management Entity (MME) and S-GW at a time, but the user equipment can have connectivity to multiple P-GWs.

**Figure 15: Major Components of the Evolved Packet Core**



The major components in the figure are:

- **E-UTRAN**—The Evolved Universal Terrestrial Radio Access Network (E-UTRAN) is the radio network portion of the LTE architecture.
- **MME**—The Mobility Management Entity (MME) is a device that manages and stores contexts for the user equipment. It generates temporary identifiers for the user equipment, manages the user equipment idle state (so the device is reachable from other devices and services), and distributes paging messages. The MME processes tracking area updates. The MME also manages security and controls bearers (the tunnels from user equipment to service).
- **Serving Gateway (S-GW)**—The S-GW handles user-plane handovers for mobility on the radio network side of the EPC and also coordinates P-GW attachments for users. When a user is roaming, at least the S-GW and MME are in the visited public land mobile network (VPLMN), whereas the P-GW can be in the HPLMN (the home routed case) or in the VPLMN (local breakout). In either case, the home network enforces subscriber authentication and policies.
- **Packet Data Network Gateway (P-GW)**—The P-GW forms the GTP tunnel endpoint for associated user equipment, allocates IP addresses, and provides support for charging and policy enforcement for service access.

- Home Subscriber Server (HSS)—The HSS is a user database that stores all subscription-related information about a user. This information supports call (connection) control and session management. The HSS function was performed by the Home Location Register (HLR) in older architectures.
- Service cloud—These are the services delivered by the Packet Data Network (PDN). This can be the global public Internet or an IP Multimedia Subsystem (IMS) network. IMS networks handle voice over IP (VoIP) calls to and from the user equipment.

The major interfaces in the figure are:

- S1—The S1 interface connects both the MME and S-GW to the mobile radio network. Technically, these are the S1-MME and S1-U interface, respectively.
- S5/S8—The S5 interface connects the P-GW with the local S-GW. When roaming, this is the S8 interface.
- S6a—The S6a interface connects the MME with the HSS. The interface is the same whether roaming or not.
- SGi (or Gi)—The SGi interface (“i” for Internet or IP) connects the P-GW to the Internet, IMS, or other IP network (such as a corporate intranet).

**Related  
Documentation**

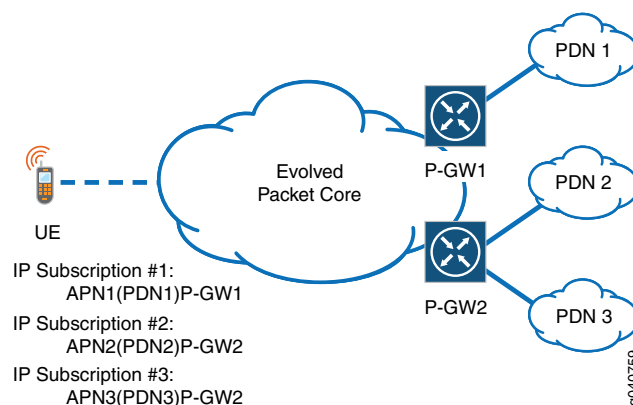
- [Overview of Mobile Networks on page 23](#)
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 25](#)
- [Overview of GGSN and P-GW on page 26](#)
- [Overview of Packet Data Network Gateway Functions on page 28](#)
- [Overview of APNs on page 32](#)
- [Overview of PDP Contexts and Bearers on page 33](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 35](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 36](#)
- [Overview of IPv6 and the Broadband Gateway on page 38](#)
- [Overview of IPv6 and the Broadband Gateway on page 38](#)
- [Serving Gateway and the S1 Interface Overview on page 39](#)
- [Serving Gateway and the S1 Interface Overview on page 39](#)
- [Service Areas and Tracking Areas Overview on page 40](#)

## Overview of APNs

In a mobile network, the access point name (APN) is the virtual private network (VPN) that connects the user equipment through the Packet Data Network Gateway (P-GW) to the Packet Data Network (PDN). User equipment can access many APNs, which are domain names and associated parameters, and one is the default APN. APNs are very similar to MPLS VPNs in landline networks.

In the Long Term Evolution (LTE) architecture for the Evolved Packet Core (EPC), the APN determines the P-GW the user equipment should use. The APN also defines the tunnel connecting the user equipment to a PDN such as the Internet. Each PDN that the user subscribes to has an APN and an associated P-GW, often called a “PDN subscription context.” One context is the default APN, connecting to a PDN such as the Internet unless the user activates another APN. [Figure 16 on page 32](#) shows the relationship among APNs, P-GWs, and packet networks.

Figure 16: APNs and the P-GW



APNs are configured by network operators and hold many of the parameters that characterize the user session to the PDN. The APN determines authorization and address allocation methods, several types of timeouts, and various other parameters. It also determines the IP address pools to be used, the charging type (such as offline or online) to be used, and the policy model (for example, if a policy and charging rules function [PCRF] is used for policy control).

The P-GW can also use various rules to determine which APN the user equipment should use. This is called the APN service selection method. The APN in turn defines the service and the P-GW that the user equipment employs.

APNs often look like Internet domain names and have two parts:

- **Network identifier**—This defines the PDN the user connects to through a P-GW. This part of the APN is mandatory. It can be as simple as **internet** or have a more complicated structure such as **juniper.net**.
- **Operator identifier**—This defines the operator whose PDN the user connects to through a P-GW. This part of the APN is optional and is often omitted. If present, it consists of the operator's Mobile Country Code (MCC) and Mobile Network Code (MNC). A more

complex APN would be something like **internet.mnc012.mcc345.gprs** or, more realistically, **Web.omnitel.it**.

**Related  
Documentation**

- [Overview of Mobile Networks on page 23](#)
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 25](#)
- [Overview of GGSN and P-GW on page 26](#)
- [Overview of Packet Data Network Gateway Functions on page 28](#)
- [Overview of the Evolved Packet Core on page 30](#)
- [Overview of PDP Contexts and Bearers on page 33](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 35](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 36](#)
- [Overview of IPv6 and the Broadband Gateway on page 38](#)
- [Overview of IPv6 and the Broadband Gateway on page 38](#)
- [Serving Gateway and the S1 Interface Overview on page 39](#)
- [Serving Gateway and the S1 Interface Overview on page 39](#)
- [Service Areas and Tracking Areas Overview on page 40](#)

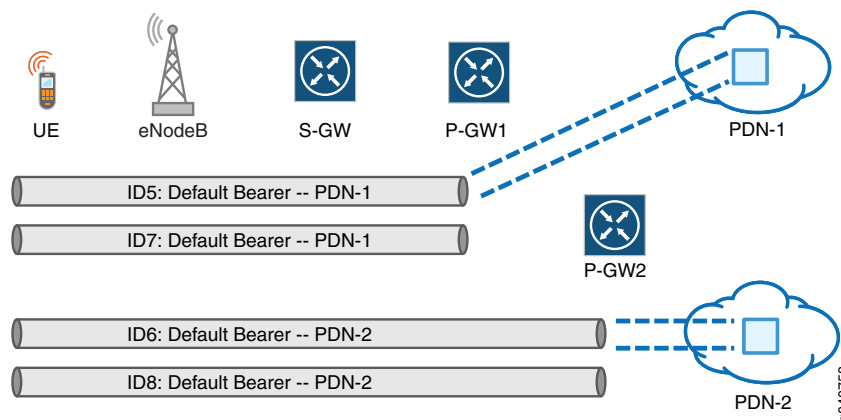
---

## Overview of PDP Contexts and Bearers

In a mobile network using the Long Term Evolution (LTE) architecture, bearers are the tunnels used to connect the user equipment to Packet Data Networks (PDNs) such as the Internet. In practice, bearers are concatenated tunnels that connect the user equipment to the PDN through the Packet Data Network Gateway (P-GW).

In older architectures, bearers were known as packet data protocol (PDP) contexts. One PDP context connects to one PDN location by default (this was the default PDP context). Other PDP contexts (up to 11) could be established to or from the same user device. The maximum of 11 still holds in 4G/LTE networks. [Figure 17 on page 34](#) shows the relationship between bearers and P-GWs.

Figure 17: Bearers, Gateways, and Packet Networks



**NOTE:** The MobileNext Broadband Gateway initially supports only default bearers.

In an LTE mobile network, one *default bearer* is established to a default P-GW whenever the user equipment device is activated (this means the user equipment is on and has performed authentication). There must be at least one default bearer to one default P-GW, but up to 11 other bearers to the same or other P-GWs can be active to a single user equipment device.

Bearers encapsulate user data with the GPRS tunneling protocol, user plane (GTP-U). The GTP-U information is in turn sent with UDP and inside IP packets.

Every user equipment device has an “always on” default bearer for each P-GW to which it connects. For example, if user equipment connects to the Internet through one P-GW and a corporate intranet through another P-GW, *two* default bearers will be active. In addition, the user equipment can establish other *dedicated bearers* to other PDNs, based on quality-of-service (QoS) requirements. For instance, viewing a streaming video over the Internet could be done over a dedicated bearer. Dedicated bearers can use a bandwidth guarantee (a guaranteed bit rate, or GBR) or the user equipment can establish a non-GBR bearer.

The bearer itself is a concatenated tunnel consisting of three portions (in a non-roaming situation), established in the following order:

- The S5 bearer—This tunnel connects the Serving Gateway (S-GW) to the P-GW. (The tunnel can extend from P-GW to PDN service network, but this is not considered here.)
- The S1 bearer—This tunnel connects the evolved NodeB (eNodeB or eNB) radio cell with the S-GW. Handover establishes a new S1 bearer for end-to-end connectivity.
- The radio bearer—This tunnel connects the user equipment to the eNodeB (eNB). This bearer follows the mobile user under the direction of the Mobile Management Entity (MME) as the radio network performs handovers when the user moves from one cell to another.



### Related Documentation

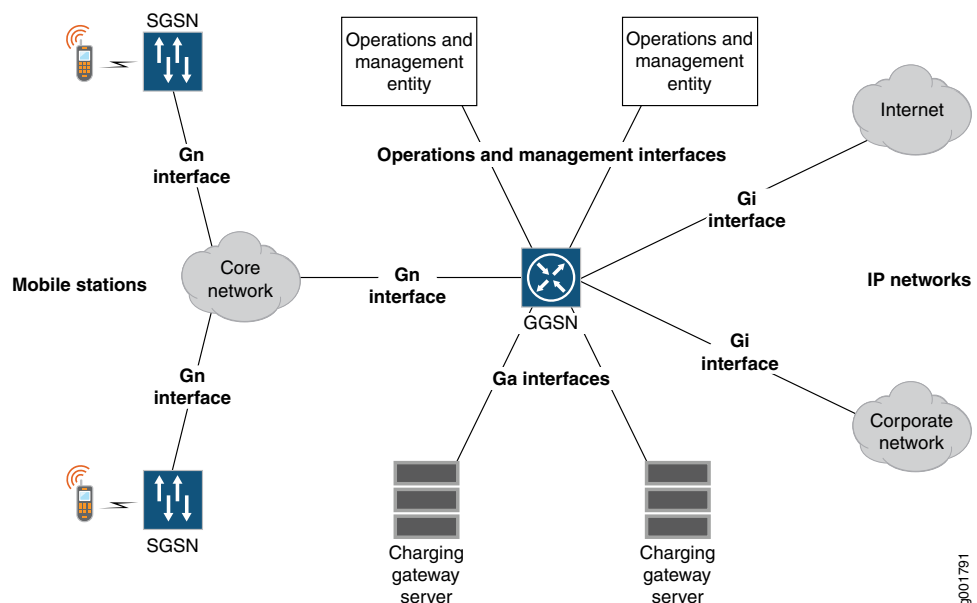
- [Overview of Mobile Networks on page 23](#)
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 25](#)
- [Overview of GGSN and P-GW on page 26](#)
- [Overview of Packet Data Network Gateway Functions on page 28](#)
- [Overview of the Evolved Packet Core on page 30](#)
- [Overview of APNs on page 32](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 35](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 36](#)
- [Overview of IPv6 and the Broadband Gateway on page 38](#)
- [Overview of IPv6 and the Broadband Gateway on page 38](#)
- [Serving Gateway and the S1 Interface Overview on page 39](#)
- [Serving Gateway and the S1 Interface Overview on page 39](#)
- [Service Areas and Tracking Areas Overview on page 40](#)

## Overview of GGSN and Broadband Gateway Deployment

The MobileNext Broadband Gateway can be configured and deployed as a gateway GPRS support node (GGSN) in a 3G network. The broadband gateway links the mobile network to various IP packet networks.

[Figure 18 on page 35](#) shows how a GGSN (the broadband gateway) is deployed in a 3G network. The devices that the GGSN connects to are shown as well.

**Figure 18: The GGSN in a 3G Network**



The GGSN supports three general types of conceptual 3G interfaces:

- Gn—These interfaces (“n” for network) connect to the mobile portion of the network, such as the Serving GPRS Support Node (SGSN). The SGSNs connect to the mobile stations themselves through the radio network.
- Gi—These interfaces (“i” for IP) connect to the IP packet portion of the network, such as the Internet or private corporate networks.
- Ga—These interfaces (“a” for administration) connect to the network management and operations portion of the network, such as the charging servers.

These defined conceptual interfaces can be implemented as almost any type of physical interface.

**Related  
Documentation**

- [Overview of Mobile Networks on page 23](#)
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 25](#)
- [Overview of GGSN and P-GW on page 26](#)
- [Overview of Packet Data Network Gateway Functions on page 28](#)
- [Overview of the Evolved Packet Core on page 30](#)
- [Overview of APNs on page 32](#)
- [Overview of PDP Contexts and Bearers on page 33](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 36](#)
- [Overview of IPv6 and the Broadband Gateway on page 38](#)
- [Overview of IPv6 and the Broadband Gateway on page 38](#)
- [Serving Gateway and the S1 Interface Overview on page 39](#)
- [Serving Gateway and the S1 Interface Overview on page 39](#)
- [Service Areas and Tracking Areas Overview on page 40](#)

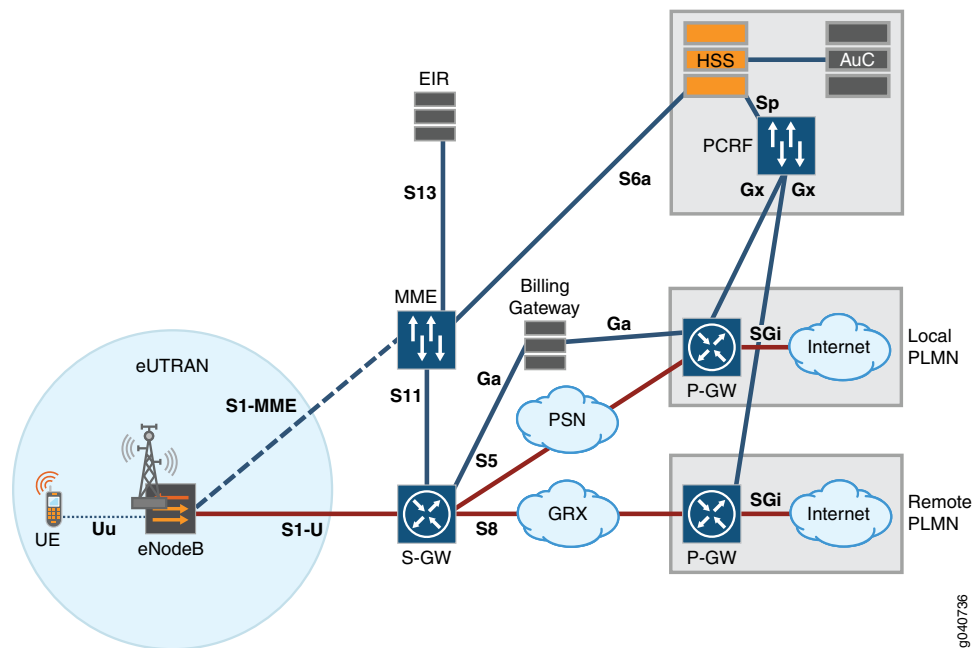
---

## Overview of 4G/LTE and Broadband Gateway Deployment

It is one thing to look at network architectures with standardized interfaces and standardized functional components. It is another to consider a realistic deployment of network components that is realistic rather than theoretical.

[Figure 19 on page 37](#) shows the major components and interfaces of a Long Term Evolution (LTE) mobile network from user equipment to network. Some of the major interfaces and components are labeled, but the emphasis here is on how these pieces are organized into a mobile network.

Figure 19: LTE Network Deployment Scenario



The major parts of the figure are:

- **eUTRAN (E-UTRAN)**—The Evolved Universal Terrestrial Radio Access Network (E-UTRAN) is the radio network portion of the LTE architecture. The user equipment is part of the E-UTRAN, as is the radio tower, or evolved NodeB (eNodeB). The Uu interface connects the user equipment to the eNodeB, and the S1 interfaces connect to the Mobility Management Entity (MME) over the S1-MME interface (for the control plane) and the Serving Gateway (S-GW) over the S1-U (for user plane) interface.
- **The HSS, AuC, and PCRF**—The Home Subscriber Server (HSS), authentication center (AuC), and policy and charging rules function (PCRF) act together to make sure that the user equipment is authorized to access a particular service or network and that the user is billed correctly for the service. The Sp interface connects the HSS to the PCRF, and the S6a interface connects the HSS to the MME. The Gx interfaces connect to the P-GWs because P-GWs enforce the policy and charging rules through the P-GW's policy and charging enforcement function (PCEF).
- **P-GW and Internet**—A grouping of P-GWs and Packet Data Network (PDN) such as the Internet form a public land mobile network (PLMN). The UE can attach to a local or HPLMN through a P-GW or through a remote PLMN when roaming (if permitted). The S5 interface connects the local P-GW to its S-GW through a packet-switched network (PSN). For roaming, the S8 interface connects the remote P-GW to its S-GW through a GPRS Roaming Exchange (GRX). Note that billing, handled by the billing gateway, is a local PLMN function (settlements are used for roaming). The Ga interface connects the P-GW and S-GW to the billing gateway.
- **S-GW, MME, EIR, and billing gateway**—These components connect the radio network to the PLMN. The MME is a device that manages user equipment information. The equipment identification register (EIR), connected to the MME over the S13 interface,

ensures that the user equipment has not been reported stolen. The MME communicates with the S-GW over the S11 interface. User authentication relates to the subscriber profile in the HSS (reached over the S6a interface). Charging information is coordinated with the billing gateway.

Together, these components (and others) make up a complete mobile network.

**Related  
Documentation**

- [Overview of Mobile Networks on page 23](#)
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 25](#)
- [Overview of GGSN and P-GW on page 26](#)
- [Overview of Packet Data Network Gateway Functions on page 28](#)
- [Overview of the Evolved Packet Core on page 30](#)
- [Overview of APNs on page 32](#)
- [Overview of PDP Contexts and Bearers on page 33](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 35](#)
- [Overview of IPv6 and the Broadband Gateway on page 38](#)
- [Serving Gateway and the S1 Interface Overview on page 39](#)
- [Serving Gateway and the S1 Interface Overview on page 39](#)
- [Service Areas and Tracking Areas Overview on page 40](#)

---

## Overview of IPv6 and the Broadband Gateway

---

The Juniper Networks MobileNext Broadband Gateway, as a Packet Data Network Gateway (P-GW) or gateway GSN (GGSN), supports IPv6 as well as IPv4. However, there are some aspects of the IPv6 support that should be detailed.

When it comes to IPv6 support, in the current release, the MobileNext Broadband Gateway:

- Supports the allocation of IPv6 addresses to the mobile device.
- Does *not* support the use of an IPv6 network to connect the MobileNext Broadband Gateway to a Serving Gateway (S-GW) in a 4G/LTE or 3G architecture.



.....

**NOTE:** This means that the GGSN or P-GW uses IPv4 addresses as internal or loopback addresses.

.....

**Related  
Documentation**

- [Overview of Mobile Networks on page 23](#)
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 25](#)
- [Overview of GGSN and P-GW on page 26](#)
- [Overview of Packet Data Network Gateway Functions on page 28](#)
- [Overview of the Evolved Packet Core on page 30](#)

- [Overview of APNs on page 32](#)
- [Overview of PDP Contexts and Bearers on page 33](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 35](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 36](#)
- [Serving Gateway and the S1 Interface Overview on page 39](#)
- [Serving Gateway and the S1 Interface Overview on page 39](#)
- [Service Areas and Tracking Areas Overview on page 40](#)

## Serving Gateway and the S1 Interface Overview

One of the main roles of the Serving Gateway (S-GW), in contrast to the Packet Data Network Gateway (P-GW), is to coordinate hand-overs among e-UTRAN Node B (eNodeB) radio cells and even, when necessary, among S-GWs and Mobility Management Entities (MMEs) through the S1 interface. The S-GW handles the GPRS tunneling protocol, control (GTP-C) and GTP, user (GTP-U) packets.

**Figure 20: S1 Interface Is Many-to-Many**

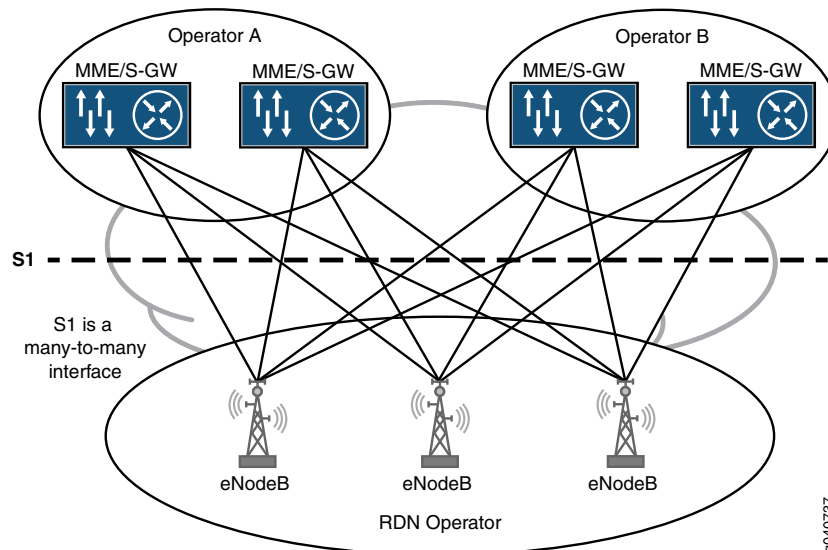


Figure 20 on page 39 shows that the S1 interface between eNodeBs and the MMEs and S-GWs is a many-to-many interface. The S1 interface supports redundancy and load sharing of these critical network nodes. Load sharing the MMEs allows the user equipment to operate in a given geographical area without changing the MME. S1 interface redundancy improves mobile network reliability. Finally, the many-to-many aspect of the S1 interface also allows the radio network to be shared by multiple operators.

### Related Documentation

- [Overview of Mobile Networks on page 23](#)
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 25](#)
- [Overview of GGSN and P-GW on page 26](#)

- [Overview of Packet Data Network Gateway Functions on page 28](#)
- [Overview of the Evolved Packet Core on page 30](#)
- [Overview of APNs on page 32](#)
- [Overview of PDP Contexts and Bearers on page 33](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 35](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 36](#)
- [Overview of IPv6 and the Broadband Gateway on page 38](#)
- [Service Areas and Tracking Areas Overview on page 40](#)
- [Serving Gateway Functions Overview on page 41](#)

## Service Areas and Tracking Areas Overview

Groups of multiple Serving Gateways (S-GWs) and Mobility Management Entities (MMEs) can be established. The MME pool area and the S-GW service area do not have to coincide. In fact, they are often different because they are established independently. If the mobile user moves between tracking areas which belong to different MME pools or S-GW pool areas, then an MME or S-GW handover will occur. So even if an MME is not changing, the S-GW can change, and even if the S-GW is not changing, the MME can change. The handovers are in addition to the inter-S-GW and inter-MME handovers.

**Figure 21: Tracking Areas and the S1 Interface**

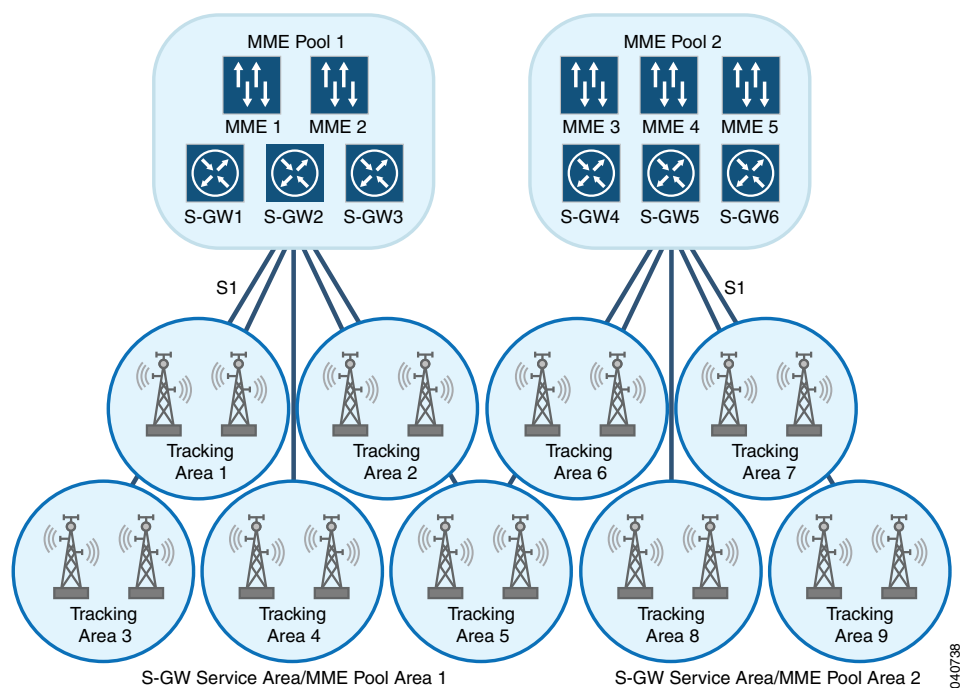


Figure 21 on page 40 shows the relationship between MME pools, S-GW serving areas (which coincide in this case), and enhanced Node B (eNodeB) tracking areas. A mobile user can move around inside the areas of this example network without changing either S-GW or MME. However, if the mobile user moves between the two tracking areas shown in the figure, both an MME hand-over and an S-GW hand-over will occur. Note the role of the S1 interface.

**Related Documentation**

- [Overview of Mobile Networks on page 23](#)
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 25](#)
- [Overview of GGSN and P-GW on page 26](#)
- [Overview of Packet Data Network Gateway Functions on page 28](#)
- [Overview of the Evolved Packet Core on page 30](#)
- [Overview of APNs on page 32](#)
- [Overview of PDP Contexts and Bearers on page 33](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 35](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 36](#)
- [Overview of IPv6 and the Broadband Gateway on page 38](#)
- [Serving Gateway and the S1 Interface Overview on page 39](#)
- [Serving Gateway Functions Overview on page 41](#)

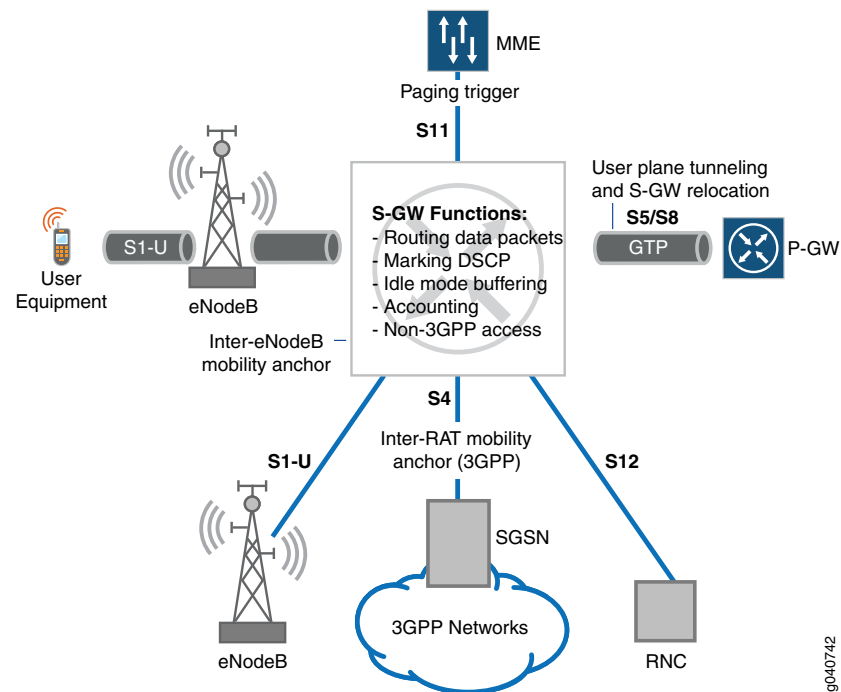
---

## Serving Gateway Functions Overview

You can configure the MobileNext Broadband Gateway as a Serving Gateway (S-GW) or Packet Data Network Gateway (P-GW), either as a standalone S-GW or standalone P-GW or collocated S-GW and P-GW.

Figure 22 on page 42 shows the broadband gateway configured as a standalone S-GW in a 4G mobile network. A mobile device only has one S-GW at any point in time.

Figure 22: S-GW Functions



The functions of the S-GW include:

- Establishing bearers based on the directives of the Mobility Management Entity (MME) over the S11 interface (bearers can be established on the S4 interface as well).
- Handling user data functions such as routing and forwarding packets to a P-GW over the S5 interface.
- Connecting the S-GW in a visitor public land mobile network (PLMN) with the P-GW in the home PLMN over the S8 interface.
- Connecting the S-GW with an enhanced Node B (eNodeB) radio network for user plane tunneling of GPRS tunneling protocol, user (GTP-U) packets and hand-overs through the S1-U interface.
- Anchoring for inter-3GPP mobility over the S4 interface connecting the S-GW with a 4G Serving GPRS Support Node (SSGN).
- Gathering accounting information per user and per bearer.

#### Related Documentation

- [Overview of Mobile Networks on page 23](#)
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 25](#)
- [Overview of GGSN and P-GW on page 26](#)
- [Overview of Packet Data Network Gateway Functions on page 28](#)
- [Overview of the Evolved Packet Core on page 30](#)
- [Overview of APNs on page 32](#)



- [Overview of PDP Contexts and Bearers on page 33](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 35](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 36](#)
- [Overview of IPv6 and the Broadband Gateway on page 38](#)
- [Serving Gateway and the S1 Interface Overview on page 39](#)
- [Service Areas and Tracking Areas Overview on page 40](#)



## CHAPTER 3

# Getting Started with Mobile Networks

- [Configuring Broadband Gateway Home PLMNs and Gateways on page 45](#)
- [Configuring Broadband Gateway Local Policies Application on page 46](#)
- [Configuring Broadband Gateway Call Rate Statistics on page 47](#)
- [Verifying the Gateway Configuration on page 48](#)
- [Configuring General Gateway Trace Options on page 49](#)
- [Configuring Mobile Options Trace Options on page 51](#)
- [Configuring Resource Manager Trace Options on page 52](#)
- [Configuring GGSN or P-GW Software Data Path Traceoptions on page 55](#)
- [Configuring an S-GW on a Broadband Gateway on page 57](#)
- [Configuring S-GW-Specific Profiles on page 58](#)
- [Configuring S-GW Traceoptions on page 59](#)
- [Configuring S-GW Software Data Path Traceoptions on page 62](#)

### Configuring Broadband Gateway Home PLMNs and Gateways

---

The MobileNext Broadband Gateway establishes a context and framework for mobile operations under the unified edge. The basic mobile framework unit is the gateway, which can be used as either a 3G gateway GPRS support node (GGSN) or 4G Packet Data Network Gateway (P-GW). The gateway also has one or more home public land mobile networks (HPLMNs) associated with it.

Before you begin configuring HPLMNs and gateways on the broadband gateway, you should have done the following:

- Configured access to the MobileNext Broadband Gateway

To establish the mobile context, configure a gateway. You also configure a list of HPLMNs that this gateway and its access point names (APNs) recognize. The HPLMNs consist of the mobile country code (MCC) and mobile network code (MNC).



**NOTE:** At initial release, the broadband gateway supports only one gateway.

To configure the gateway and HPLMN list:

1. Configure a name for the gateway.

```
[edit unified-edge gateways ggsn-pgw ]  
user@host# set MGB1
```



**NOTE:** You can include dashes or underscores, but many special characters are not allowed in the gateway name.

2. Configure a list of HPLMNs for the gateway.

```
[edit unified-edge gateways ggsn-pgw MBG1]  
user@host# set home-plmn mcc 001 mnc 01
```



**NOTE:** The MMC/MNC combination 00101 is reserved for test networks.

**Related  
Documentation**

- [Understanding Mobile User Types on page 12](#)
- [Configuring Broadband Gateway Local Policies Application on page 46](#)
- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Configuring General Gateway Trace Options on page 49](#)
- [Configuring Mobile Options Trace Options on page 51](#)
- [Configuring Resource Manager Trace Options on page 52](#)

---

## Configuring Broadband Gateway Local Policies Application

The MobileNext Broadband Gateway associates a number of locally configured policies with a configured gateway. These policies are used for connection admission control and service-related parameters.

Before you begin configuring local policies on the broadband gateway, you should have done the following:

- Configured access to the MobileNext Broadband Gateway

You configure the local policies at the **[edit unified-edge cos-cac]** hierarchy level and apply the profiles at the **[edit unified-edge local-policies local-policies-name]** hierarchy level. You can configure many policy profiles, but you can apply only one of each type at a time to the gateway as a whole.

To associate the gateway with local policy profiles:

1. Use a name for the local policies profile.

```
[edit unified-edge local-policies local-policy-profile-1]
```

2. Associate the gateway with a classifier profile by user type.

```
[edit unified-edge local-policies local-policy-profile-1]
user@host# set classifier-profile home-classifier-profile-1
user@host# set roamer-classifier-profile roamer-classifier-profile-1
user@host# set visitor-classifier-profile visitor-classifier-profile-1
```

3. Associate the gateway with a class-of-service policy profiles by user type.

```
[edit unified-edge local-policies local-policy-profile-1]
user@host# set policy-profile home-classifier-policy-profile-1
user@host# set roamer-policy-profile roamer-classifier-policy-profile-1
user@host# set visitor-policy-profile visitor-policy-profile-1
```

4. Associate the gateway with the resource threshold profile used to define admission control for managing system overload conditions.

```
[edit unified-edge local-policies local-policy-profile-1]
user@host# set resource-threshold-profiles resource-threshold-profile-1
```

5. Associate the gateway with the downlink bandwidth pool.

```
[edit unified-edge local-policies local-policy-profile-1]
user@host# set dl-bandwidth-pool bw-pool-downlink-1
```

6. Associate the gateway with the uplink bandwidth pool.

```
[edit unified-edge local-policies local-policy-profile-1]
user@host# set ul-bandwidth-pool bw-pool-uplink-1
```

#### Related Documentation

- [Understanding Mobile User Types on page 12](#)
- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Configuring General Gateway Trace Options on page 49](#)
- [Configuring Mobile Options Trace Options on page 51](#)
- [Configuring Resource Manager Trace Options on page 52](#)

## Configuring Broadband Gateway Call Rate Statistics

The MobileNext Broadband Gateway records statistics about the rate of calls through the gateway. You can configure parameters relating to the recording of these statistics at the gateway level.

Before you begin configuring call rate statistics on the broadband gateway, you should have done the following:

- Configured a list of home public land mobile networks (HPLMNs) and a gateway on the MobileNext Broadband Gateway

To configure the option values for call rate statistics:

1. Configure the history interval value for collecting call rate statistics.

```
[edit unified-edge gateways ggsn-pgw MBG1 call-rate-statistics]
user@host# set history 10
```



**NOTE:** Enter a value from 1 through 20 intervals to keep call rate statistics.

2. Configure the interval for collecting call rate statistics.

```
[edit unified-edge gateways ggsn-pgw MBG1 call-rate-statistics]  
user@host# set interval 5
```



**NOTE:** Enter a value in minutes from 5 through 120 minutes.

**Related  
Documentation**

- [Configuring Broadband Gateway Home PLMNs and Gateways on page 45](#)
- [Configuring General Gateway Trace Options on page 49](#)
- [Configuring Mobile Options Trace Options on page 51](#)
- [Configuring Resource Manager Trace Options on page 52](#)

---

## Verifying the Gateway Configuration

**Purpose** Display information about the gateway configuration.

- Action**
- To display information about the call rate and general statistics on the gateway:

```
user@host> show unified-edge ggsn-pgw call-rate statistics  
user@host> show unified-edge ggsn-pgw statistics
```

- To clear information about the general statistics on the gateway:

```
user@host> clear unified-edge ggsn-pgw statistics
```

- To display information about the status of the gateway:

```
user@host> show unified-edge ggsn-pgw status  
user@host> show unified-edge ggsn-pgw status preemption-list
```

- To clear information about the subscriber peers on the gateway:

```
user@host> clear unified-edge ggsn-pgw subscribers peer
```

- To display information about the resources on the gateway:

```
user@host> show unified-edge ggsn-pgw resource-manger clients
```

**Related  
Documentation**

- [Configuring Broadband Gateway Home PLMNs and Gateways on page 45](#)
- [Configuring Broadband Gateway Local Policies Application on page 46](#)
- [Configuring Broadband Gateway Call Rate Statistics on page 47](#)

## Configuring General Gateway Trace Options

General gateway tracing operations record detailed messages about the operation of configured gateways on the MobileNext Broadband Gateway.

General gateway trace options are related to overall gateway operation. You can specify which trace operations are logged by including specific tracing flags and levels.

[Table 3 on page 49](#) describes the flags relating to the mobile unified edge that you can include at the `[edit unified-edge gateways ggsn-pgw gateway-name traceoptions flag]` hierarchy level.

**Table 3: General Gateway Trace Flags**

Flag	Description
<b>all</b>	Trace everything.
<b>bulkjob</b>	Trace resources.
<b>config</b>	Trace configuration events.
<b>cos-cac</b>	Trace CoS and CAC events.
<b>ctxt</b>	Trace user equipment, PDN, or bearer context events.
<b>fsm</b>	Trace FSM events.
<b>gtpu</b>	Trace GTP-U events.
<b>ha</b>	Trace high availability events.
<b>init</b>	Trace events related to protocol daemon initialization.
<b>pfem</b>	Trace PFE manager events.
<b>stats</b>	Trace stats events.
<b>waitq</b>	Trace waitq events.

[Table 4 on page 49](#) describes the levels you can include.

**Table 4: Trace Levels**

Level	Description
<b>all</b>	Match all levels.
<b>error</b>	Match error conditions.
<b>info</b>	Match informational messages.

Table 4: Trace Levels (*continued*)

notice	Match conditions that should be specially handled.
verbose	Match verbose messages.
warning	Match warning messages.

To configure tracing options for general gateway events:

1. Specify that you want to configure tracing options for general gateway events.

```
[edit unified-edge gateways ggsn-pgw gateway-name ]
user@host# edit traceoptions
```

2. Configure the filename for the trace file.

```
[edit unified-edge gateways ggsn-pgw gateway-name traceoptions]
user@host# set file general-gw-log
```

3. (Optional) Configure the maximum size of each trace file.

```
[edit unified-edge gateways ggsn-pgw gateway-name traceoptions]
user@host# set file size 100m
```



**NOTE:** When a trace file (for example, gateway-log) reaches its maximum size, it is renamed gateway-log.0, then gateway-log.1, and so on, until the maximum number of trace files is reached. The oldest archived file is then overwritten.

4. Configure the tracing flag.

```
[edit unified-edge gateways ggsn-pgw gateway-name traceoptions]
user@host# set flag all
```



**NOTE:** Use care when tracing all operations on a gateway. This can have a performance impact.

5. Configure the tracing level.

```
[edit unified-edge gateways ggsn-pgw gateway-name traceoptions]
user@host# set level error
```

6. View the trace file.

```
user@host# file show /var/log/gateway-log
```

#### Related Documentation

- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Configuring Broadband Gateway Home PLMNs and Gateways on page 45](#)
- [Configuring Broadband Gateway Local Policies Application on page 46](#)
- [Configuring Mobile Options Trace Options on page 51](#)



- [Configuring Resource Manager Trace Options on page 52](#)

## Configuring Mobile Options Trace Options

Mobile options tracing operations record detailed messages about the operation of unified edge options on the MobileNext Broadband Gateway. Mobile options trace options are related to the processor daemon operation. You can specify which trace operations are logged by including specific tracing flags.

[Table 5 on page 51](#) describes the flags relating to the mobile unified edge that you can include at the `[edit unified-edge mobile-options traceoptions flag]` hierarchy level.

**Table 5: Mobile Options Trace Flags**

Flag	Description
<b>all</b>	Trace everything.
<b>configuration</b>	Trace configuration events.
<b>error</b>	Trace events related to catastrophic errors in the daemon.
<b>init</b>	Trace events related to protocol daemon initialization.
<b>protocol</b>	Trace protocol processing events.

To configure tracing options for mobile options:

1. Specify that you want to configure tracing options for mobile options.

```
[edit unified-edge mobile-options]
user@host# edit traceoptions
```

2. Configure the filename for the trace file.

```
[edit unified-edge mobile-options traceoptions]
user@host# set file mobile-options-log
```

3. (Optional) Configure the maximum size of each trace file.

```
[edit unified-edge mobile-options traceoptions]
user@host# set file size 100m
```



**NOTE:** When a trace file (for example, *mobile-log*) reaches its maximum size, it is renamed *mobile-log.0*, then *mobile-log.1*, and so on, until the maximum number of trace files is reached. The oldest archived file is then overwritten.

4. Configure the tracing flag.

```
[edit unified-edge mobile-options traceoptions]
user@host# set flag all
```



**NOTE:** Use care when tracing all operations on a gateway. This can have a performance impact.

5. View the trace file.

```
user@host# file show /var/log/mobile-options-log
```

#### Related Documentation

- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Configuring Broadband Gateway Home PLMNs and Gateways on page 45](#)
- [Configuring Broadband Gateway Local Policies Application on page 46](#)
- [Configuring General Gateway Trace Options on page 49](#)
- [Configuring Resource Manager Trace Options on page 52](#)

## Configuring Resource Manager Trace Options

Resource management tracing operations record detailed messages about the operation of resource management clients and server on the MobileNext Broadband Gateway.



**NOTE:** You do not configure the resource manager for the broadband gateway. The process runs automatically.

Resource management trace options are divided into flags for the resource management *server* (the active Routing Engine) and the resource management *client* (the session Dense Port Concentrators [DPCs] and interface DPCs and Modular Port Concentrators [MPCs]). You can set server and client flags independently. You can specify which trace operations are logged by including specific tracing flags and levels.

[Table 6 on page 52](#) describes the flags relating to the resource management server that you can include at the **[edit unified-edge resource-management server traceoptions flag]** hierarchy level.

**Table 6: Resource Management Server Trace Flags**

Flag	Description
<b>all</b>	Trace everything.
<b>communication</b>	Trace Infra code.
<b>config</b>	Trace configuration code.
<b>gres</b>	Trace GRES code.
<b>info-manager</b>	Trace information management code.
<b>init</b>	Trace events related to data path daemon initialization.

Table 6: Resource Management Server Trace Flags (*continued*)

<b>memory</b>	Trace memory management code.
<b>packet-steering</b>	Trace packet-steering code.
<b>resource-manager</b>	Trace resource management code.
<b>signal</b>	Trace signal handling code.
<b>state</b>	Trace state handling code.
<b>timer</b>	Trace timer code.
<b>ui</b>	Trace user interface code.

Table 7 on page 53 describes the flags relating to the resource management client that you can include at the **[edit unified-edge resource-management client traceoptions flag]** hierarchy level.

Table 7: Resource Management Client Trace Flags

Flag	Description
<b>all</b>	Trace everything.
<b>communication</b>	Trace IPC code.
<b>info-tables</b>	Trace information table code.
<b>infra</b>	Trace FSM and Infra code.
<b>memory</b>	Trace memory management code.
<b>redundancy</b>	Trace GRES code.
<b>resource-tables</b>	Trace resource table code.

Table 8 on page 53 describes the levels you can include.

Table 8: Trace Levels

Level	Description
<b>all</b>	Match all levels.
<b>error</b>	Match error conditions.
<b>info</b>	Match informational messages.
<b>notice</b>	Match conditions that should be specially handled.

Table 8: Trace Levels (*continued*)

<b>verbose</b>	Match verbose messages.
<b>warning</b>	Match warning messages.

To configure tracing options for resource management operations:

1. Specify that you want to configure tracing options for resource management client or server operations.

```
[edit unified-edge resource-management server]
[edit unified-edge resource-management client]
user@host# edit traceoptions
```

2. Configure the filename for the trace file.

```
[edit unified-edge resource-management server traceoptions]
[edit unified-edge resource-management client traceoptions]
user@host# set file rm-log
```

3. (Optional) Configure the maximum size of each trace file.

```
[edit unified-edge resource-management server traceoptions]
[edit unified-edge resource-management client traceoptions]
user@host# set file size 100m
```



**NOTE:** When a trace file (for example, rm-log) reaches its maximum size, it is renamed rm-log.0, then rm-log.1, and so on, until the maximum number of trace files is reached. The oldest archived file is then overwritten.

4. Configure the tracing flag.

```
[edit unified-edge resource-management server traceoptions]
[edit unified-edge resource-management client traceoptions]
user@host# set flag all
```



**NOTE:** Use care when tracing all operations on a gateway. This can have a performance impact.

5. Configure the tracing level.

```
[edit unified-edge resource-management server traceoptions]
[edit unified-edge resource-management client traceoptions]
user@host# set level error
```

6. View the trace file.

```
user@host# file show /var/log/rm-log
```

#### Related Documentation

- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Configuring Broadband Gateway Home PLMNs and Gateways on page 45](#)
- [Configuring Broadband Gateway Local Policies Application on page 46](#)

- [Configuring General Gateway Trace Options on page 49](#)
- [Configuring Mobile Options Trace Options on page 51](#)

## Configuring GGSN or P-GW Software Data Path Traceoptions

Data path tracing operations record detailed messages about the operation of services such as packet reassembly or IPv6 router advertisements on the MobileNext Broadband Gateway. You can trace various types of data path operations such as configuration events, memory usage, the age of a packet flow, configuration information, and other information. You can specify which trace operations are logged by including specific tracing flags and levels.

[Table 9 on page 55](#) describes the flags relating to the data path that you can include at the `[edit unified-edge gateways ggsn-pgw gateway-name software-datapath traceoptions flag]` hierarchy level.

**Table 9: Trace Flags**

Flag	Description
<code>ager</code>	Trace flow ager.
<code>all</code>	Trace everything.
<code>commands</code>	Trace operational commands.
<code>configuration</code>	Trace configuration events.
<code>flow</code>	Trace flow.
<code>init</code>	Trace events related to data path daemon initialization.
<code>ipv6-router-advertisement</code>	Trace IPv6 router advertisement.
<code>memory</code>	Trace memory.
<code>reassembly</code>	Trace reassembly.
<code>redundancy</code>	Trace redundancy.

[Table 10 on page 55](#) describes the levels you can include.

**Table 10: Trace Levels**

Level	Description
<code>all</code>	Match all levels.
<code>error</code>	Match error conditions.
<code>info</code>	Match informational messages.

Table 10: Trace Levels (*continued*)

notice	Match conditions that should be specially handled.
verbose	Match verbose messages.
warning	Match warning messages.

To configure tracing options for data path operations:

1. Specify that you want to configure tracing options for data path operations.

```
[edit unified-edge gateways ggsn-pgw MBG1 software-datapath]
user@host# edit traceoptions
```

2. Configure the filename for the trace file.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 software-datapath traceoptions]
user@host# set file datapath-log
```

3. (Optional) Configure the maximum size of each trace file.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 software-datapath traceoptions]
user@host# set file size 100m
```



**NOTE:** When a trace file (for example, data-path-log) reaches its maximum size, it is renamed data-path-log.0, then data-path-log.1, and so on, until the maximum number of trace files is reached. The oldest archived file is then overwritten.

4. Configure the tracing flag.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 software-datapath traceoptions]
user@host# set flag all
```



**NOTE:** You should use care when tracing all operations on a gateway. This can have a performance impact.

5. Configure the tracing level.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 software-datapath traceoptions]
user@host# set level error
```

6. View the trace file.

```
user@host# file show /var/log/data-path-log
```

#### Related Documentation

- [Understanding the Broadband Gateway Software Data Path on page 10](#)
- [Configuring S-GW Software Data Path Traceoptions on page 62](#)

## Configuring an S-GW on a Broadband Gateway

The MobileNext Broadband Gateway establishes a context and framework for mobile operations under the unified edge. The basic mobile framework unit is the gateway, which can be used as a Serving Gateway (S-GW). The S-GW also has one or more home public land mobile networks (HPLMNs) associated with it.

Before you begin configuring an S-GW on the broadband gateway, you should have done the following:

- Configured access to the MobileNext Broadband Gateway

To establish the mobile context for the S-GW, you name the gateway, configure a list of HPLMNs, and set various other parameters. The HPLMNs consist of the mobile country code (MCC) and mobile network code (MNC).

To configure the gateway and related parameters:

1. Configure a name for the gateway.

```
[edit unified-edge gateways sgw ]
user@host# set MGB-SGW1
```



**NOTE:** You can include dashes or underscores, up to 63 characters, but many special characters are not allowed in the gateway name.

2. Configure a list of HPLMNs for the gateway.

```
[edit unified-edge gateways sgw MBG-SGW1]
user@host# set home-plmn mcc 001 mnc 01
```



**NOTE:** The MMC/MNC combination 00101 is reserved for test networks.

3. (Option) Set idle mode buffering expiration timer on the gateway.

```
[edit unified-edge gateways sgw MBG-SGW1]
user@host# set idle-mode-buffering expire-timer 60
```



**NOTE:** By default, idle mode buffering is enabled. You can set the expiration timer to any value from 30 through 300 seconds. If you disable idle-mode buffering, the 1G memory is used for subscriber management.

4. (Option) Enable remote delete on peer failure on the gateway.

```
[edit unified-edge gateways sgw MBG-SGW1 ]
user@host# set remote-delete-on-peer-fail
```



**NOTE:** By default, the S-GW will not delete peers on failure.

5. (Option) Configure the maximum bearers allowed on the gateway.

```
[edit unified-edge gateways sgw MBG-SGW1 ]
user@host# set maximum-bearers 500000
```



**NOTE:** By default, the S-GW supports 12,000,000 bearers. You can set any value from 100000 through 12000000.

6. (Option) Enable preemption on the gateway to allow some bearers to pre-empt others.

```
[edit unified-edge gateways sgw MBG-SGW1 ]
user@host# set preemption enable
```



**NOTE:** By default, the S-GW does not perform preemption.

**Related  
Documentation**

- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Serving Gateways and the MobileNext Broadband Gateway Overview on page 12](#)
- [Overview of Standalone S-GW User Plane Packet Flow on page 16](#)
- [Overview of Collocated Gateways: Control Plane on page 19](#)
- [Overview of Collocated Gateways: User Plane on page 20](#)
- [Configuring S-GW-Specific Profiles on page 58](#)
- [Configuring S-GW Traceoptions on page 59](#)

---

## Configuring S-GW-Specific Profiles

The MobileNext Broadband Gateway Serving Gateway (S-GW) uses two profile statements. This topic shows how to configure the profile statements that are unique to the S-GW configuration.

Before you begin configuring S-GW profiles on the broadband gateway, you should have done the following:

- Configured the chassis of the MobileNext Broadband Gateway
- Configured the interfaces used by the MobileNext Broadband Gateway
- Configured the IP reassembly parameters and local policy profiles referenced by the S-GW configuration

To establish the IP reassembly and local policy profiles for the S-GW, you apply the profile to the S-GW. The use of these profiles is optional.

To configure profiles for the S-GW:

1. Optionally, configure the S-GW IP reassembly profile.

```
[edit unified-edge gateways sgw MBG-SGW1]
```



```
user@host# set ip-reassembly-profile ip-reassembly--one
```



**NOTE:** The IP reassembly parameters such as timeout are configured for the profile at the [edit services ip-reassembly] hierarchy level.

2. Optionally, configure the S-GW local policy profile.

```
[edit unified-edge gateways sgw MBG-SGW1]
user@host# set local-policy-profile local-profile-1
```



**NOTE:** The local policy profile parameters must already be configured at the [edit unified-edge] hierarchy level. Only the classifier-profile and resource-threshold-profiles are supported on the S-GW.

#### Related Documentation

- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Serving Gateways and the MobileNext Broadband Gateway Overview on page 12](#)
- [Overview of Standalone S-GW User Plane Packet Flow on page 16](#)
- [Overview of Collocated Gateways: Control Plane on page 19](#)
- [Overview of Collocated Gateways: User Plane on page 20](#)
- [Configuring an S-GW on a Broadband Gateway on page 57](#)
- [Configuring S-GW Traceoptions on page 59](#)

## Configuring S-GW Traceoptions

Serving Gateway (S-GW) tracing operations record detailed messages about the operation of high-level S-GW services on the MobileNext Broadband Gateway. You can trace various types of operations such as configuration events, connection admission control events, PFE manager events, and other information. You can specify which trace operations are logged by including specific tracing flags and levels.

[Table 11 on page 59](#) describes the flags relating to the S-GW that you can include at the [edit unified-edge gateways sgw gateway-name traceoptions flag] hierarchy level.

**Table 11: S-GW Trace Flags**

Flag	Description
all	Trace everything.
bulkjob	Trace resources.
config	Trace configuration events.
cos-cac	Trace class-of-service and connection admission control events.

Table 11: S-GW Trace Flags (*continued*)

<b>ctxt</b>	Trace user equipment, packet data network, and bearer context events.
<b>fsm</b>	Trace finite state machine events.
<b>gtpu</b>	Trace GPRS tunneling protocol, user (GTP-U) protocol events.
<b>ha</b>	Trace high availability events.
<b>init</b>	Trace initialization events.
<b>pfem</b>	Trace Packet Forwarding Engine manager events.
<b>stats</b>	Trace statistic events.
<b>waitq</b>	Trace wait queue events.

[Table 12 on page 60](#) describes the levels you can include.

Table 12: S-GW Trace Levels

Level	Description
<b>all</b>	Match all levels.
<b>error</b>	Match error conditions.
<b>info</b>	Match informational messages.
<b>notice</b>	Match conditions that should be specially handled.
<b>verbose</b>	Match verbose messages.
<b>warning</b>	Match warning messages.

To configure tracing options for S-GW operations:

1. Specify that you want to configure tracing options for S-GW operations.

```
[edit unified-edge gateways sgw MBG2 ]
user@host# edit traceoptions
```



**NOTE:** You can use the `no-remote-trace` statement at this level to disable remote tracing capabilities.

2. Configure the filename for the trace file.

```
[edit unified-edge gateways sgw MBG2 traceoptions]
user@host# set file datapath-log
```

3. (Optional) Configure the maximum size of each trace file.

```
[edit unified-edge gateways sgw MBG2 traceoptions]
user@host# set file size 100m
```



**NOTE:** When a trace file (for example, `sgw-log`) reaches its maximum size, it is renamed `sgw-log.0`, then `sgw-log.1`, and so on, until the maximum number of trace files is reached. The oldest archived file is then overwritten.

4. Configure the tracing flag.

```
[edit unified-edge gateways sgw MBG2 traceoptions]
user@host# set flag all
```



**NOTE:** You should use care when tracing all operations on a gateway. This can have a performance impact.

5. Configure the tracing level.

```
[edit unified-edge gateways sgw MBG2 traceoptions]
user@host# set level error
```

6. View the trace file.

```
user@host# file show /var/log/sgw-log
```

**Related  
Documentation**

- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Serving Gateways and the MobileNext Broadband Gateway Overview on page 12](#)
- [Overview of Standalone S-GW User Plane Packet Flow on page 16](#)
- [Overview of Collocated Gateways: Control Plane on page 19](#)
- [Overview of Collocated Gateways: User Plane on page 20](#)
- [Configuring an S-GW on a Broadband Gateway on page 57](#)
- [Configuring S-GW-Specific Profiles on page 58](#)
- [Configuring S-GW Software Data Path Traceoptions on page 62](#)
- [Configuring S-GW GTP Traceoptions on page 338](#)
- [Configuring S-GW Charging Traceoptions on page 448](#)
- [Configuring S-GW Local Persistent Storage Traceoptions on page 451](#)

## Configuring S-GW Software Data Path Traceoptions

Data path tracing operations record detailed messages about the operation of Serving Gateway (S-GW) services on the MobileNext Broadband Gateway. You can trace various types of data path operations such as packet reassembly, IPv6 router advertisements, memory usage, configuration events, and other information. You can specify which trace operations are logged by including specific tracing flags and levels.

Table 13 on page 62 describes the flags relating to the data path that you can include at the `[edit unified-edge gateways sgw gateway-name software-datapath traceoptions flag]` hierarchy level.

Table 13: S-GW Data Path Trace Flags




Flag	Description
<code>ager</code>	Trace flow ager.
<code>all</code>	Trace everything.
<code>commands</code>	Trace operational commands.
<code>configuration</code>	Trace configuration events.
<code>flow</code>	Trace flow.
<code>init</code>	Trace events related to data path daemon initialization.
<code>ipv6-router-advertisement</code>	Trace IPv6 router advertisement.
<code>memory</code>	Trace memory.
<code>reassembly</code>	Trace reassembly.
<code>redundancy</code>	Trace redundancy.

Table 14 on page 62 describes the levels you can include.

Table 14: S-GW Datapath Trace Levels

Level	Description
<code>all</code>	Match all levels.
<code>error</code>	Match error conditions.
<code>info</code>	Match informational messages.
<code>notice</code>	Match conditions that should be specially handled.
<code>verbose</code>	Match verbose messages.

Table 14: S-GW Datapath Trace Levels (*continued*)

warning	Match warning messages.
To configure tracing options for data path operations:	
1. Specify that you want to configure tracing options for data path operations.	
[edit unified-edge gateways sgw MBG2 software-datapath]	
user@host# edit traceoptions	
	<b>NOTE:</b> You can use the <code>no-remote-trace</code> statement at this level to disable remote tracing capabilities.
2. Configure the filename for the trace file.	
[edit unified-edge mobile gateways sgw MBG2 software-datapath traceoptions]	
user@host# set file datapath-log	
3. (Optional) Configure the maximum size of each trace file.	
[edit unified-edge mobile gateways sgw MBG2 software-datapath traceoptions]	
user@host# set file size 100m	
	<b>NOTE:</b> When a trace file (for example, <code>data-path-log</code> ) reaches its maximum size, it is renamed <code>data-path-log.0</code> , then <code>data-path-log.1</code> , and so on, until the maximum number of trace files is reached. The oldest archived file is then overwritten.
4. Configure the tracing flag.	
[edit unified-edge mobile gateways sgw MBG2 software-datapath traceoptions]	
user@host# set flag all	
	<b>NOTE:</b> You should use care when tracing all operations on a gateway. This can have a performance impact.
5. Configure the tracing level.	
[edit unified-edge mobile gateways sgw MBG2 software-datapath traceoptions]	
user@host# set level error	
6. View the trace file.	
user@host# file show /var/log/datapath-log	
<b>Related Documentation</b>	• <a href="#">Understanding the Broadband Gateway Software Data Path on page 10</a>
	• <a href="#">Configuring GGSN or P-GW Software Data Path Traceoptions on page 55</a>
	• <a href="#">Configuring S-GW Traceoptions on page 59</a>



## PART 2

# System Configuration

- [Configuring Mobility on MX 3D Devices on page 67](#)
- [Configuring Redundancy on MX 3D Devices on page 77](#)
- [Configuring IP Reassembly on page 91](#)





## CHAPTER 4

# Configuring Mobility on MX 3D Devices

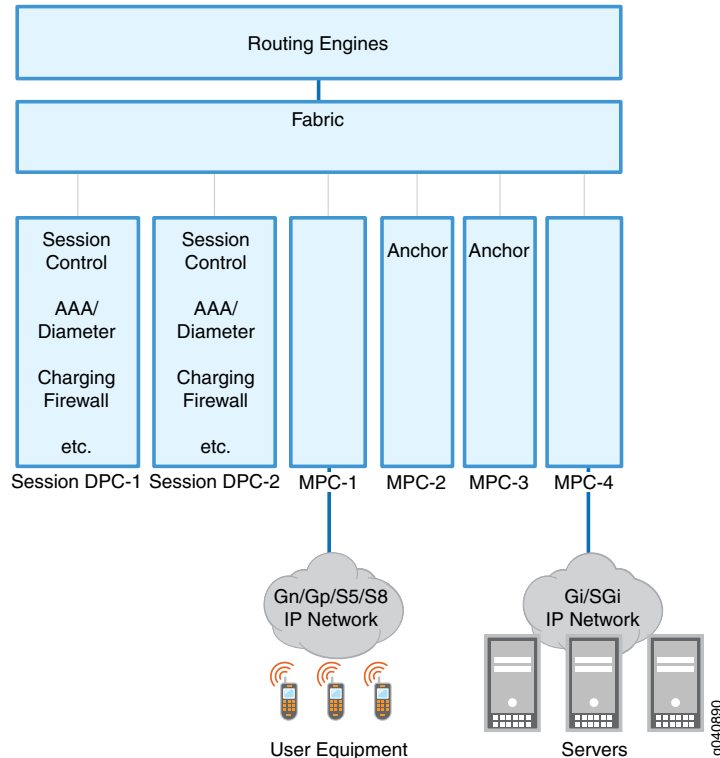
- [MobileNext Broadband Gateway Chassis Overview on page 68](#)
- [Configuring Session DPCs for Mobility on page 70](#)
- [Configuring Interface DPCs or MPCs for User Mobility Traffic on page 72](#)
- [Understanding the MobileNext Broadband Gateway Anchors on page 73](#)
- [Configuring Anchor Session DPCs and PFEs on page 75](#)
- [Verifying the MobileNext Broadband Gateway Chassis Configuration on page 76](#)

## MobileNext Broadband Gateway Chassis Overview

You should begin MobileNext Broadband Gateway configuration with basic chassis configuration. Whether you used the broadband gateway as a gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW), determining the number of service and interface cards running the mobility package will make it easier to complete software configuration. Also, the relationship between physical devices such as Modular Port Concentrator (MPC) ports and logical constructs such as access point names (APNs) is not always obvious on the broadband gateway.

The broadband gateway consists of Routing Engines (we recommend two), session Dense Port Concentrators (DPCs) (we recommend two or more), and interface DPCs or MPCs (we recommend two or more). The interface DPCs and MPCs house the input and output Packet Forwarding Engine and physical interfaces. Other service DPCs and interface cards can be installed, but only the elements configured to run the mobility software package can be part of the broadband gateway function. In other words, some elements of the broadband gateway might not be involved in mobile packet flows at all, but these elements implement a provider edge (PE) router function, related network address translation (NAT) or IP security (IPsec) services, and so on. This topic describes only the mobile portion of the configuration. In [Figure 23 on page 68](#), the session DPCs are shown on the left and the interface boards are shown as MPCs on the right.

**Figure 23: Session DPCs and Interfaces on the Broadband Gateway**



This chassis configuration overview covers:

- [Session DPCs for Mobility on page 69](#)
- [Overview of Mobility Interface Types on page 69](#)

## Session DPCs for Mobility

The session Dense Port Concentrators (DPCs) are multiservices DPCs that are used for mobile purposes. Incoming control packets from user equipment using the GPRS tunneling protocol, control (GTP-C) tunneling protocol are sent to one of these session DPCs. The selected session DPC becomes the *anchor* session DPC for this particular flow of packets. All control packets (GTP-C packets) relating to the session are sent to this anchor device.

The mobile services performed by the session DPC include:

- Session control
- Authentication, authorization, and accounting (AAA) checking using the Diameter protocol
- Charging parameters
- Admission control functions

## Overview of Mobility Interface Types

The interfaces that allow GPRS tunneling protocol, user plane (GTP-U) messages to flow into and out of the MobileNext Broadband Gateway can be Modular Port Concentrators (MPCs) or Dense Port Concentrators (DPCs). These mobile interfaces are configured as regular device interfaces; for example, **ge-0/1/2**, where the first position digit indicates the FPC slot (0), the second position digit indicates the PIC (Packet Forwarding Engine) position (1), and the last digit indicates the physical port (2). Some or all of the interface cards can be configured as anchor DPCs or MPCs. Once a session is established with the GTP-C control packets, all uplink and downlink user packets sent with the GTP-U tunnel protocol flow through the designated anchor device.

Examples of mobile interface DPCs or MPCs include:

- Mobile 60-Gigabit Ethernet Enhanced Queuing MPC
- Mobile 10-Gigabit Ethernet MPC with SFP+

The above list is for illustration only and is not an exclusive or comprehensive list.

### Related Documentation

- [Configuring Session DPCs for Mobility on page 70](#)
- [Configuring Interface DPCs or MPCs for User Mobility Traffic on page 72](#)
- [Understanding the MobileNext Broadband Gateway Anchors on page 73](#)
- [Configuring Anchor Session DPCs and PFEs on page 75](#)
- [Verifying the MobileNext Broadband Gateway Chassis Configuration on page 76](#)
- [Overview of Broadband Gateway System Architecture on page 3](#)

## Configuring Session DPCs for Mobility

---

The MobileNext Broadband Gateway chassis has a number of open slots for cards (also called boards). Once installed, the cards must be configured. This topic describes the configuration process for the mobility FPC slots that hold session Dense Port Concentrators (DPCs).

Before you begin, you should have done the following:

- Installed the broadband gateway
- Installed the cards in the broadband gateway
- Decided which slots will be used for mobility

The session DPC cards of the broadband gateway must run in 64-bit mode. To simplify the configuration process, the broadband gateway software includes a predefined **mobility** group. This group includes all the parameters required for stable system operation. You apply the **mobility** group to the session DPC slots in the same way you apply any Junos OS group.

The predefined **mobility** group contains the following statements:

```
[edit groups]
mobility {
  chassis {
    fpc <*> {
      pic <*> {
        adaptive-services {
          service-package {
            extension-provider {
              boot-os embedded-junos64;
              control-cores 1;
              data-pollers 1;
              object-cache-size 512;
              package jservices-mobile;
              total-wired-memory 14336;
              wired-max-processes 8;
              wired-process-memory-size 1024;
            }
          }
        }
      }
    }
  }
}
```



**NOTE:** These parameters promote stable system operation. You should *not* change these parameters except under the advice of JTAC.

To configure a session DPC for mobility services, you load the default configuration file and merge it with your configuration, then apply the predefined **mobility** group to the session DPC. This task assumes that the session DPC is installed in chassis slot 1 and that both PICs are used for mobility services.

1. Load and merge the **mobility-defaults.conf** file.

```
[edit]
user@host# load merge /etc/config/mobility-defaults.conf
```

2. Configure the **mobility** group to run on both PICs in FPC 0.

```
[edit chassis]
user@host# set fpc 0 pic 0 apply-groups mobility
user@host# set fpc 0 pic 1 apply-groups mobility
```



**NOTE:** You must include every services PIC configured with the `jservices-mobile` package at the `[edit unified-edge gateways ggsn-pgw gateway-name system anchor-spics]` hierarchy level on the broadband gateway. If you do not include the services PIC as an anchor, then the services PIC will not be used by the broadband gateway.

---

**Related  
Documentation**

- [MobileNext Broadband Gateway Chassis Overview on page 68](#)
- [Configuring Interface DPCs or MPCs for User Mobility Traffic on page 72](#)
- [Understanding the MobileNext Broadband Gateway Anchors on page 73](#)
- [Configuring Anchor Session DPCs and PFEs on page 75](#)
- [Verifying the MobileNext Broadband Gateway Chassis Configuration on page 76](#)
- [Overview of Broadband Gateway System Architecture on page 3](#)

---

## Configuring Interface DPCs or MPCs for User Mobility Traffic

---

The MobileNext Broadband Gateway chassis has a number of open slots for cards (also called boards). Once installed, the cards must be configured. This topic describes the configuration process for the interface Modular Port Concentrators (MPCs) or Dense Port Concentrators (DPCs) used for user mobile traffic.

Before you begin, you should have done the following:

- Installed the MobileNext Broadband Gateway
- Installed the cards of the broadband gateway
- Decided which DPCs or MPCs will be used for user mobility traffic

To configure an interface DPC or MPC for user mobility traffic, you configure the DPC or MPC to run the mobility forwarding package. You can configure this capability at the card (FPC) or Packet Forwarding Engine level. To configure the DPC or MPC:

1. Configure the forwarding package at the FPC level (so that all Packet Forwarding Engines understand what to do with mobility packets) by configuring the **mobility ggsn-pgw** (for a GGSN or P-GW) forwarding package or the **mobility sgw** (for a S-GW) forwarding package at the FPC level.

```
[edit chassis]
user@host# set fpc 0 forwarding-packages mobility ggsn-pgw
user@host# set fpc 0 forwarding-packages mobility sgw
```

In this example, all Packet Forwarding Engines on the DPC or MPC in FPC slot 0 are configured for mobility traffic.

2. Optionally, configure the forwarding package at the PIC level, so that *only* this PIC understands what to do with mobility packets by configuring the **mobility ggsn-pgw** or **mobility sgw** forwarding package at the PIC level:

```
[edit chassis]
user@host# set fpc 0 pfe 0 forwarding-packages mobility ggsn-pgw
user@host# set fpc 0 pfe 0 forwarding-packages mobility sgw
```

In this example, only Packet Forwarding Engine 0 on the DPC or MPC in FPC slot 0 is configured for mobility traffic.



**NOTE:** You must include every Packet Forwarding Engine configured with the `ggsn-pgw` forwarding package or `sgw` forwarding package at the `[edit unified-edge gateways ggsn-pgw gateway-name system anchor-pfes]` hierarchy level on the broadband gateway. If you do not specify the Packet Forwarding Engine as an anchor, then the Packet Forwarding Engine will not be used by the broadband gateway.

#### Related Documentation

- [Configuring Session DPCs for Mobility on page 70](#)
- [Configuring Anchor Session DPCs and PFEs on page 75](#)
- [Verifying the MobileNext Broadband Gateway Chassis Configuration on page 76](#)

## Understanding the MobileNext Broadband Gateway Anchors

The MobileNext Broadband Gateway processes GPRS tunneling protocol (GTP) and IP packets as they make their way upstream from mobile device to IP network or downstream from IP network to mobile device. Both control and data GTP packets are processed by an *anchor* session Dense Port Concentrator (DPC) or Packet Forwarding Engine (which are part of an interface DPC or Modular Port Concentrator [MPC] inside the broadband gateway). Anchor session PICs or Packet Forwarding Engines can be configured in a redundant manner to provide a failover data path in case of hardware problems.

Session DPCs use 1:1 redundancy and the component PICs (session DPCs have two PICs) are essentially configured in pairs to provide backup. For example, you can configure `ams0` so that PIC 1 in FPC slot 5 backs up PIC 1 in FPC slot 4. In other words, `mams-5/1/0` backs up `mams-4/1/0`. However, this configuration alone does not make `ams0` (or `mams-4/1/0`) an anchor session DPC. A separate configuration step is required for that. This “anchor or not” capability allows session DPCs to be used for services other than mobility.

The same logic applies to interface DPCs or MPCs (Packet Forwarding Engines), except that the redundancy is N:1. In this case, you can configure `apfe0` so that `pfe-9/0/0` is a warm standby for `pfe-7/0/0` and `pfe-8/0/0`. However, another configuration step is required to make the Packet Forwarding Engines in FPC slot 7 and 8 anchor Packet Forwarding Engines.

Figure 24: Upstream GTP-U Traffic

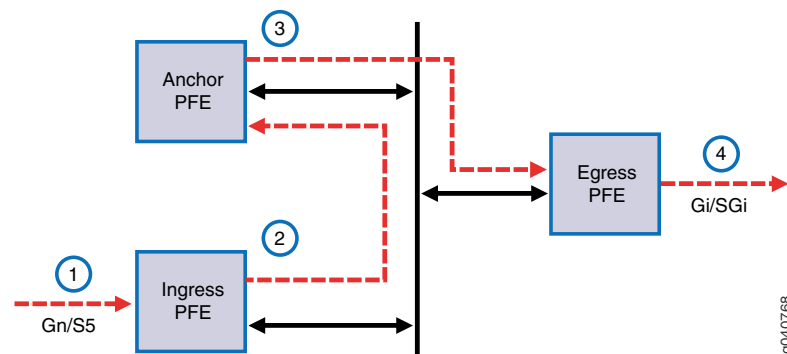


Figure 24 on page 74 shows how all GPRS tunneling protocol, user plane (GTP-U) traffic traverses an anchor Packet Forwarding Engine upstream from a Gn or S5 interface to a Gi or SGi interface:

- The arriving GTP-U packet is filtered by the outer IP address and associated with the proper Virtual Routing and Forwarding (VRF) table .
- The packet is sent to the anchor Packet Forwarding Engine associated with that group tunnel endpoint identifier (TEID) in the GTP header.
- The packet is decapsulated and the TEID is processed. The correct charging and quality-of-service (QoS) parameters are applied and the inner IP address is used for a route table lookup. The packet is sent to the correct egress interface.
- The packet is sent out on the correct Gi or SGi interface (other service functions such as network address translation [NAT] might be applied).

The downstream GTP-U packet process is a mirror of the upstream process.

Figure 25: Downstream GTP-U Traffic

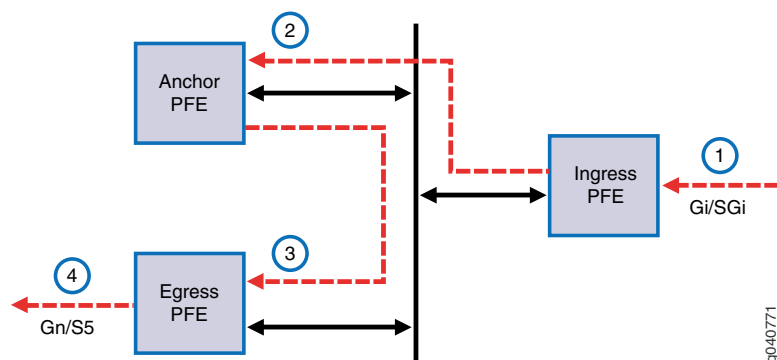




Figure 24 on page 74 shows how all GTP-U traffic traverses an anchor Packet Forwarding Engine downstream from a Gi or SGi interface to a Gn or S5 interface:

- The arriving IP packet is looked up in the route table associated with the proper virtual routing and forwarding table (VRF).
- The packet is sent to the anchor Packet Forwarding Engine associated with that route.
- The TEID associated with the packet is processed and the correct charging and QoS parameters are applied. The packet is then encapsulated with the TEID and the outer IP address. The outer IP address in the GTP header is used for a route lookup for the SGSN or S-GW. The packet is sent to the egress interface.
- The packet is sent from the correct Gn or S5 interface.

#### Related Documentation

- [Configuring Anchor Session DPCs and PFEs on page 75](#)
- [MobileNext Broadband Gateway Chassis Overview on page 68](#)
- [Configuring Session DPCs for Mobility on page 70](#)
- [Configuring Interface DPCs or MPCs for User Mobility Traffic on page 72](#)
- [Verifying the MobileNext Broadband Gateway Chassis Configuration on page 76](#)

## Configuring Anchor Session DPCs and PFEs

Even with redundancy configured, a separate step is required to make a session Dense Port Concentrator (DPC) or Packet Forwarding Engine (Packet Forwarding Engines are part of an interface DPC or Modular Port Concentrator [MPC]) a mobility anchor. An anchor acts as a tunnel endpoint for control and data GPRS tunneling protocol (GTP) packets.

Before you begin configuring anchors on a broadband gateway, you should have done the following:

- Configured the chassis of the MobileNext Broadband Gateway
- Configured the interfaces of the broadband gateway
- (Optional) Configured the general redundancy parameters for the broadband gateway

To determine the anchor session DPCs (PICs) and Packet Forwarding Engines, you configure the components as anchors.

To configure anchor session DPCs (PICs):

1. Add the PIC to the list of **anchor-spics**.

```
[edit unified-edge gateway ggsn-pgw MBG1 system]
user@host# set anchor-spics interface ams0
```



**NOTE:** You can set the anchor PICs individually if you do not have redundancy configured. For example, you can use `ms-1/1/0` instead of `ams0`.

2. Add the Packet Forwarding Engine to the list of **anchor-pfes**.

```
[edit unified-edge gateway ggsn-pgw MBG1 system]
user@host# set anchor-pfes interface apfe0
user@host# set anchor-pfes interface apfe1
```



**NOTE:** You can set the anchor Packet Forwarding Engines individually if you do not have redundancy configured. For example, you can use `pfe-4/1/0` and `pfe-4/2/0`.

**Related  
Documentation**

- [Configuring Session DPCs for Mobility on page 70](#)
- [Configuring Interface DPCs or MPCs for User Mobility Traffic on page 72](#)
- [Verifying the MobileNext Broadband Gateway Chassis Configuration on page 76](#)

---

## Verifying the MobileNext Broadband Gateway Chassis Configuration

---

**Purpose**    Display information about the MobileNext Broadband Gateway chassis configuration.

**Action**    • To display information about the chassis:

```
user@host> show chassis hardware
```

**Related  
Documentation**

- [Configuring Session DPCs for Mobility on page 70](#)
- [Configuring Interface DPCs or MPCs for User Mobility Traffic on page 72](#)
- [Configuring Anchor Session DPCs and PFEs on page 75](#)

## CHAPTER 5

# Configuring Redundancy on MX 3D Devices

- [Broadband Gateway Redundancy Overview on page 78](#)
- [Configuring Session DPC Redundancy on page 80](#)
- [Configuring Interface Redundancy on page 82](#)
- [Understanding the Broadband Gateway Anchor Failover Behavior on page 84](#)
- [Example: Configuring Broadband Gateway Redundancy on page 86](#)

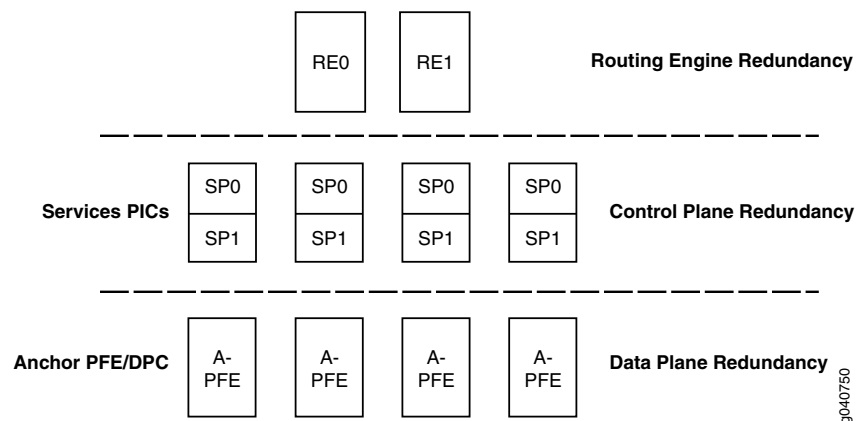
## Broadband Gateway Redundancy Overview

The MobileNext Broadband Gateway chassis contains Routing Engines, session Dense Port Concentrators (DPCs), and interface DPCs or Modular Port Concentrators (MPCs) (housing PFEs). Whether used as a GPRS gateway support node (GGSN) or Packet Data Network Gateway (P-GW), service and interface cards running the mobility package are configured to provide redundancy similar to that between the Routing Engines. However, different types of redundancy are used for the different levels of hardware used in the broadband gateway.

The broadband gateway consists of Routing Engines (we recommend two), sessions DPCs (we recommend two or more), and interface PFEs (we recommend two or more DPCs or MPCs). Other service DPCs and interface cards can be installed, but only the elements configured to run the mobility software package can be part of the broadband gateway function. In other words, some elements of the broadband gateway might not be involved in mobile packet flows, but they implement a provider edge (PE) router function, related network address translation (NAT) or IPsec services, and so on. This topic describes only the mobile redundancy portion of the configuration.

Figure 26 on page 78 shows that redundancy is available for the Routing Engines, session DPCs, and interface PFEs (housed in interface DPCs or MPCs). However, there are important differences in each type.

**Figure 26: Redundancy Available on the Broadband Gateway**



This redundancy configuration overview covers:

- [Routing Engine Redundancy on page 78](#)
- [Session DPC Redundancy on page 79](#)
- [Interface Redundancy on page 80](#)

### Routing Engine Redundancy

The Routing Engine is an Intel-based PCI platform that runs the Junos OS software on all product lines. The software processes that run on the Routing Engine oversee all of the functions that perform the mobility tasks running on the chassis. On the MobileNext

Broadband Gateway, there is 1:1 redundancy on the Routing Engines when two (the maximum) are installed.

When two Routing Engines are installed in the broadband gateway, both are powered on, but only one is active (the master). At boot time, both Routing Engines run an arbitration algorithm and elect one as master. The second Routing Engine is in standby mode and performs no functions. If the master Routing Engine fails, the standby unit takes over.

By default, the master Routing Engine is **RE0**. You can change the default master by including the appropriate **routing-engine** statement at the **[edit chassis redundancy]** hierarchy level.



**NOTE:** Although you can run the broadband gateway with only one Routing Engine, we do not recommend it.

The Routing Engine components are hot-pluggable. Removal or failure of the standby does not affect the function of the broadband gateway.

However, if the master Routing Engine is removed from the chassis:

- If there is only one Routing Engine, then packet forwarding halts until the Routing Engine is reinstalled and functioning normally.
- If there are two Routing Engines, packet forwarding halts while the standby Routing Engine becomes the master.

You can configure the broadband gateway so that the standby Routing Engine automatically becomes the master if it stops receiving keepalive signals from the original master. You can also configure automatic switchover for other problems on the master, such as a hard disk failure. For more information, see the section about Routing Engine redundancy in the *Junos OS System Basics Configuration Guide*.

## Session DPC Redundancy

The MobileNext Broadband Gateway chassis includes a number of session DPCs (we recommend at least two). Each session DPC consists of two services PICs: services PIC 0 (SP0) and services PIC 1 (SP1). The session DPCs anchor control plane functions on the broadband gateway. The anchor DPC can be an individual PIC or aggregate.

The session DPCs support 1:1 redundancy. That is, the PICs in the session DPCs are configured in a one-to-one correspondence with their backups. So, for example, if the PIC0 in the session DPC in FPC slot 0 is paired with PIC0 in the session DPC in FPC slot 1, one PIC will back up the other PIC. These pairs are called aggregate multiservices (**ams-**) DPCs. However, the standby device is lost as a services DPC and all services are supplied by the active DPC PIC. In this case, the session DPC PICs associate **ams-0/0/0** and **ams-1/0/0**. You also configure units for AMS interfaces, and these are used for AAA and charging.



**NOTE:** You cannot configure a services PIC logical interface (`ms-0/0/0.0`, for example) if you also make the same logical interface part of an AMS group (`ams-0/0/0.0` for example). This configuration will not commit.

You configure the AMS member interface that is the preferred backup.

## Interface Redundancy

The MobileNext Broadband Gateway chassis includes a number of interface Packet Forwarding Engines housed on DPCs or MPCs (we recommend at least two DPCs or MPCs). Each Packet Forwarding Engine consists of two or four Packet Forwarding Engines, depending on the DPC or MPC type. These are PFE0 and PFE1 (or optionally, PFE2 and PFE3). Some Packet Forwarding Engines are designated as anchor devices, and keep various parameters for the data plane traffic flow. Packets related to a particular flow must be processed by an anchor Packet Forwarding Engine. The anchor Packet Forwarding Engine can be a single Packet Forwarding Engine or an aggregate.

The interface Packet Forwarding Engines offer N:1 redundancy. That is, a configured number of interface Packet Forwarding Engines (N) are backed up by one warm standby Packet Forwarding Engine. Optionally, you can group Packet Forwarding Engines for redundancy purposes so that each member of the group shares the same fate.

To configure redundancy, you select a list of interface Packet Forwarding Engines to place on the active (primary) list. Then you select a different Packet Forwarding Engine to act as the secondary (standby) Packet Forwarding Engine for all Packet Forwarding Engines in the active group.

### Related Documentation

- [Configuring Session DPC Redundancy on page 80](#)
- [Configuring Interface Redundancy on page 82](#)
- [Understanding the Broadband Gateway Anchor Failover Behavior on page 84](#)
- [Example: Configuring Broadband Gateway Redundancy on page 86](#)
- [Configuring Anchor Session DPCs and PFEs on page 75](#)

---

## Configuring Session DPC Redundancy

The MobileNext Broadband Gateway chassis includes a number of session Dense Port Concentrators (DPCs) (we recommend at least two). Each session DPC consists of two services PICs: services PIC 0 and services PIC 1. The session DPCs anchor control plane functions on the broadband gateway.

Before you begin configuring session DPC redundancy on a broadband gateway chassis, you should have done the following:

- Configured the chassis of the broadband gateway
- Configured the session DPCs

The session DPCs support 1:1 redundancy. That is, the PICs in the session DPCs are configured in a one-to-one correspondence with their backups. So, for example, if the PIC0 in the session DPC in FPC slot 0 is paired with PIC0 in the session DPC in FPC slot 1, one PIC will back up the other PIC. These pairs are called aggregate multiservices (**ams-**) PICs and the member interfaces are called members of the AMS (**mams-**). However, the standby device is lost as a services PIC and all services are supplied by the active PIC. In this case, the session PICs associate **mams-0/0/0** and **mams-1/0/0** as active and standby pairs. You also configure units for AMS interfaces, and these are used for AAA and charging.



**NOTE:** You cannot configure a services PIC logical interface (**ms-0/0/0.0**, for example) if you also make the same logical interface part of an AMS (**mams-0/0/0.0**, for example). This configuration will not commit.

You configure the AMS member interface that is the preferred backup. You can configure more than one AMS group, but each must have the 1:1 redundancy, of course.

To configure AMS group membership and redundancy actions for a pair of session DPCs on a broadband gateway:

1. Configure the session DPC redundancy pair called **ams0** so that PIC 1 of the session DPC in FPC slot 0 is backed-up by FPC slot 5 PIC 1.

[edit interfaces]

```
user@host# set ams0 load-balancing-options member-interface mams-4/1/0
user@host# set ams0 load-balancing-options member-interface mams-5/1/0
```



**NOTE:** The **load-balancing-options** keyword has nothing to do with load balancing. When used for mobility, session DPCs automatically load-balance sessions.

2. Configure the preferred backup for **ams0** so that FPC 4 PIC 1 is the active session DPC and FPC 5 PIC 1 is the backup.

[edit interfaces]

```
user@host# set ams0 load-balancing-options high-availability-options many-to-one
preferred-backup mams-5/1/0
```



**NOTE:** The **many-to-one** option is still used for 1:1 redundancy in this case.

3. Configure the logical interfaces (units) for **ams0** so that **unit 0** and **unit 1** are available for AAA and charging uses.

[edit interfaces]

```
user@host# set ams0 unit 1 family inet
user@host# set ams0 unit 2 family inet
```



**NOTE:** You do not have to assign an IP address.

4. Configure the failure parameters for the members on **ams0**.

[edit interfaces]

```
user@host# set ams0 load-balancing-options member-interface-options  
redistribute-all-traffic enable-rejoin
```



**NOTE:** The *enable-rejoin* option is the only option currently supported for *redistribute-all-traffic*. If you configure the *redistribute-all-traffic* statement, you cannot also configure the *drop-member-traffic* statement on the same AMS group.

**Related  
Documentation**

- [Broadband Gateway Redundancy Overview on page 78](#)
- [Configuring Interface Redundancy on page 82](#)
- [Understanding the Broadband Gateway Anchor Failover Behavior on page 84](#)
- [Example: Configuring Broadband Gateway Redundancy on page 86](#)
- [Configuring Anchor Session DPCs and PFEs on page 75](#)

---

## Configuring Interface Redundancy

The MobileNext Broadband Gateway chassis includes a number of interface Packet Forwarding Engines housed on Dense Port Concentrators (DPCs) or Modular Port Concentrators (MPCs) (we recommend at least two DPCs or MPCs). Each Packet Forwarding Engine consists of two or four Packet Forwarding Engines, depending on the DPC or MPC type. These are PFE0 and PFE1 (or optionally, PFE2 and PFE3). Some Packet Forwarding Engines are designated as anchor devices, and keep various parameters for the data plane traffic flow. Packets related to a particular flow must be processed by an anchor Packet Forwarding Engine.

Before you begin configuring session DPC redundancy on a broadband gateway chassis, you should have done the following:

- Configured the chassis of the broadband gateway
- Configured the interface DPCs or MPCs used for mobility

The interface Packet Forwarding Engines offer N:1 redundancy. That is, a configured number of interface Packet Forwarding Engines (N) are backed up by one warm standby Packet Forwarding Engine. Optionally, you can group Packet Forwarding Engines for redundancy purposes so that each member of the group shares the same fate.

To configure interface redundancy for mobility, you select a list of interface Packet Forwarding Engines to place on the active (primary) list. Then you select a different Packet Forwarding Engine to act as the secondary (standby) Packet Forwarding Engine for all Packet Forwarding Engines in the active group.

You cannot configure a secondary Packet Forwarding Engine to share a FPC (first interface configuration parameter) with any of its primary Packet Forwarding Engines.



In other words, the following is *not* a valid configuration because the secondary **pfe-2/1/0** shares an FPC with primary **pfe-2/0/0**:

- Primary: **pfe-1/0/0**
- Primary: **pfe-2/0/0**
- Primary: **pfe-3/0/0**
- Secondary: **pfe-2/1/0**

On the other hand, the following *is* a valid configuration because the secondary **pfe-2/1/0** does *not* share an FPC with any primary:

- Primary: **pfe-0/1/0**
- Primary: **pfe-0/2/0**
- Primary: **pfe-1/2/0**
- Secondary: **pfe-2/1/0**

To configure group membership and redundancy actions for a number of interface DPCs or MPCs on a broadband gateway:

1. Configure the interface DPC or MPC redundancy list called **apfe1** with a Packet-Forwarding-Engine-by-Packet-Forwarding-Engine list of redundant components.

[edit interfaces]

```
user@host# set apfe1 anchoring-options primary-list pfe-7/0/0
user@host# set apfe1 anchoring-options primary-list pfe-8/0/0
user@host# set apfe1 anchoring-options secondary pfe-9/0/0
user@host# set apfe1 anchoring-options warm-standby
```



**NOTE:** The warm-standby option is the only mode currently supported. In this configuration (for example), ge-7/0/0 or ge-8/0/0 is backed up by ge-9/0/0 in case of failure, but not ge-7/1/0.

2. Optionally, you can configure a group name for Packet-Forwarding-Engine-level redundancy **apfe1** and **apfe2** so that all components share the same fate.

[edit interfaces]

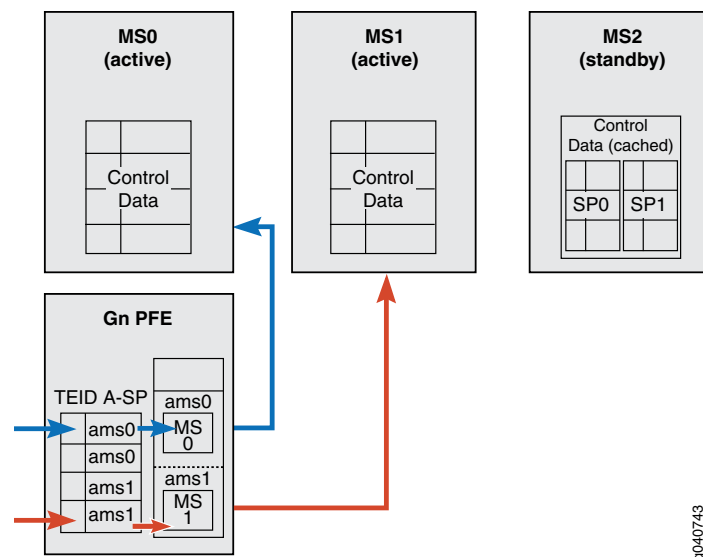
```
user@host# set apfe1 apfe-group-set apfe-group-name1
user@host# set apfe1 anchoring-options primary-list pfe-7/0/0
user@host# set apfe1 anchoring-options primary-list pfe-8/0/0
user@host# set apfe1 anchoring-options secondary pfe-9/0/0
user@host# set apfe1 anchoring-options warm-standby
user@host# set apfe2 apfe-group-set apfe-group-name1
user@host# set apfe2 anchoring-options primary-list pfe-7/2/0
user@host# set apfe2 anchoring-options primary-list pfe-8/2/0
user@host# set apfe2 anchoring-options secondary pfe-9/2/0
user@host# set apfe2 anchoring-options warm-standby
```

- Related Documentation**
- [Broadband Gateway Redundancy Overview on page 78](#)
  - [Configuring Session DPC Redundancy on page 80](#)
  - [Understanding the Broadband Gateway Anchor Failover Behavior on page 84](#)
  - [Example: Configuring Broadband Gateway Redundancy on page 86](#)
  - [Configuring Anchor Session DPCs and PFEs on page 75](#)

## Understanding the Broadband Gateway Anchor Failover Behavior

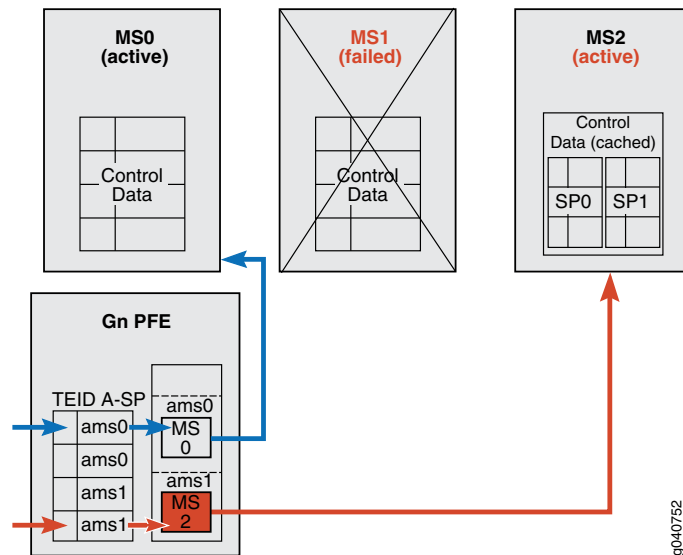
The MobileNext Broadband Gateway anchor session Dense Port Concentrators (DPCs) (housing PICs) and interface PFEs can be configured for redundancy. However, due to the different nature of the redundancy involved, 1:1 for anchor session PICs and N:1 for anchor interface PFEs, the failover behavior is slightly different.

**Figure 27: Control Plane Anchor Operation Before Failure**



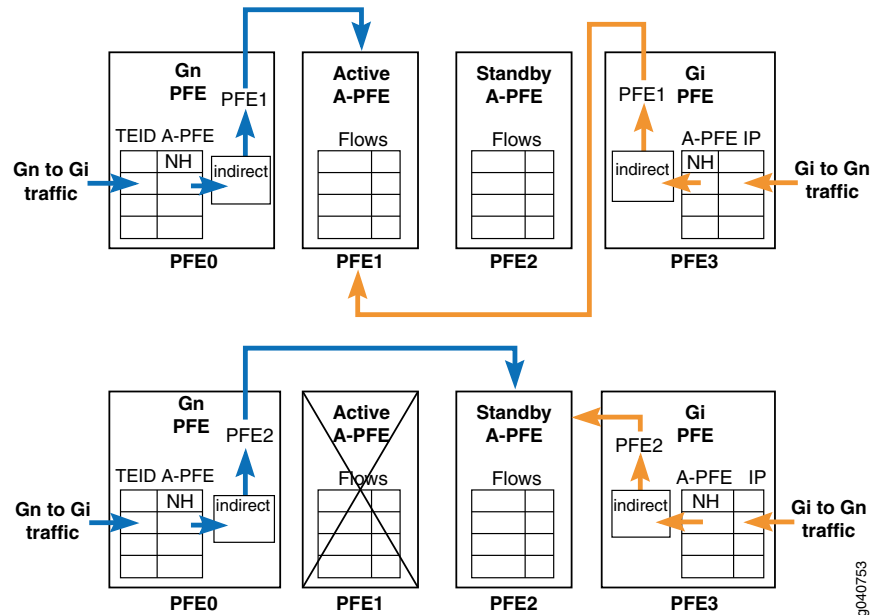
As shown in [Figure 27 on page 84](#), you can configure session DPCs with or without backup. In this case, **MS0** has no backup redundancy, while both PICs (PIC0 and PIC1) on **MS1** are backed up 1:1 by standby **MS2**. When the anchor session DPC **MS1** fails, packets cannot be processed strictly by hardware data path until the transfer of control to the new anchor is complete. This is shown in [Figure 28 on page 85](#). Note that **ams1** now points to **MS2**, the new active anchor.

Figure 28: Control Plane Anchor Operation After Failure



However, data plane packets feature N:1 anchor data path redundancy. Both pre- and post-failure Packet Forwarding Engine data paths are shown in [Figure 29 on page 85](#). For clarity, only the active and standby Packet Forwarding Engines are shown.

Figure 29: Pre- and Post-Failure PFE Datapaths



During the transition on the ingress and egress interface Packet Forwarding Engines sending data plane packets from the failed PFE1 to the new active PFE2, packets cannot be processed strictly by hardware data path until the transfer of control to the new anchor is complete.

- Related Documentation**
- [Broadband Gateway Redundancy Overview on page 78](#)
  - [Configuring Session DPC Redundancy on page 80](#)
  - [Configuring Interface Redundancy on page 82](#)
  - [Example: Configuring Broadband Gateway Redundancy on page 86](#)
  - [Configuring Anchor Session DPCs and PFEs on page 75](#)

---

## Example: Configuring Broadband Gateway Redundancy

This example shows how to configure redundancy for a MobileNext Broadband Gateway chassis containing session Dense Port Concentrators (DPCs) and interface DPCs and Module Port Concentrators (MPCs) (housing Packet Forwarding Engines). Routing Engine redundancy is not unique to mobility and is not discussed in this example. This topic describes only the unique mobile redundancy portion of the configuration.

- [Requirements on page 86](#)
- [Overview on page 86](#)
- [Configuration on page 88](#)
- [Verification on page 90](#)

### Requirements

This example uses the following hardware and software components:

- An MX chassis equipped with four session DPCs and three interface DPCs or MPCs.
- Junos OS Mobility package

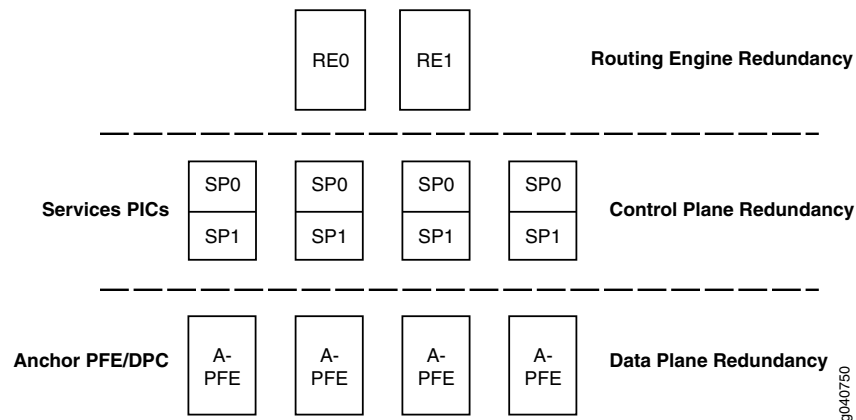
Before you begin:

- Install the chassis hardware.
- Configure the chassis.

### Overview

[Figure 30 on page 87](#) shows a broadband gateway chassis with multiple Routing Engines (not discussed further in this example), session DPCs, and interfaces Packet Forwarding Engines (housed in DPCs or MPCs).

Figure 30: Redundancy Example for the Broadband Gateway



In this example, the chassis has session DPCs in slots 4 and 5 featuring 1:1 redundancy. Group **ams0** will backup PIC **mams-4/1/0** with **mams-5/1/0** and redistribute all traffic with the rejoin option. Group **ams1** will back up PIC **mams-4/0/0** with **mams-5/0/0**. Both groups have two logical units for authentication, authorization, and accounting (AAA) and charging. The chassis also has interface DPCs or MPCs in Packet Forwarding Engines slots 7, 8, and 9, featuring N:1 redundancy, in this case, 2:1. Packet Forwarding Engine **pfe-9/0/0** backs up (using warm standby) Packet Forwarding Engines **pfe-7/0/0** and **pfe-8/0/0**.

You cannot configure a secondary Packet Forwarding Engine to share a FPC (first interface configuration parameter) with any of its primary Packet Forwarding Engines.

In other words, the following *is not* a valid configuration because the secondary Packet Forwarding Engine **pfe-2/1/0** shares an FPC with the primary Packet Forwarding Engine **pfe-2/0/0**:

- Primary: **pfe-1/0/0**
- Primary: **pfe-2/0/0**
- Primary: **pfe-3/0/0**
- Secondary: **pfe-2/1/0**

On the other hand, the following *is* a valid configuration because the secondary Packet Forwarding Engine **pfe-2/1/0** does *not* share an FPC with any primary Packet Forwarding Engines:

- Primary: **pfe-0/1/0**
- Primary: **pfe-0/2/0**
- Primary: **pfe-1/2/0**
- Secondary: **pfe-2/1/0**

## Configuration

Redundancy for the above is configured by:

- [Configuration on page 88](#)

---

### Configuration

#### CLI Quick Configuration

```
[edit interfaces]
user@host# set ams0 load-balancing-options member-interface mams-4/1/0
user@host# set ams0 load-balancing-options member-interface mams-5/1/0
user@host# set ams0 load-balancing-options high-availability-options many-to-one
  preferred-backup mams-5/1/0
user@host# set ams0 load-balancing-options member-failure-options
  redistribute-all-traffic enable-rejoin
user@host# set ams0 unit 1 family inet
user@host# set ams0 unit 2 family inet
user@host# set ams1 load-balancing-options member-interface mams-4/0/0
user@host# set ams1 load-balancing-options member-interface mams-5/0/0
user@host# set ams1 load-balancing-options high-availability-options many-to-one
  preferred-backup mams-5/0/0
user@host# set ams1 unit 1 family inet
user@host# set ams1 unit 2 family inet

user@host#set apfe0 anchoring-options primary-list pfe-7/0/0
user@host#set apfe0 anchoring-options primary-list pfe-8/0/0
user@host#set apfe0 anchoring-options secondary pfe-9/0/0
user@host#set apfe0 anchoring-options warm-standby
```

#### Step-by-Step Procedure

To configure redundancy on the broadband gateway:

1. Configure the Aggregated Multiservices (AMS) interface **ams0** and specify the interface behavior in case of failure of the active member.  

```
[edit interfaces]
user@host# set ams0 load-balancing-options member-interface mams-4/1/0
user@host# set ams0 load-balancing-options member-interface mams-5/1/0
user@host# set ams0 load-balancing-options high-availability-options many-to-one
  preferred-backup mams-5/1/0
user@host# set ams0 load-balancing-options member-failure-options
  redistribute-all-traffic enable-rejoin
user@host# set ams0 unit 1 family inet
user@host# set ams0 unit 2 family inet
```
2. Configure the AMS interface **ams1**.  

```
[edit interfaces]
user@host# set ams1 load-balancing-options member-interface mams-4/0/0
user@host# set ams1 load-balancing-options member-interface mams-5/0/0
user@host# set ams1 load-balancing-options high-availability-options many-to-one
  preferred-backup mams-5/0/0
user@host# set ams1 unit 1 family inet
user@host# set ams1 unit 2 family inet
```
3. Configure the primary and secondary Packet Forwarding Engines of the aggregated Packet Forwarding Engine **apfe0** and configure redundancy in warm standby mode.

```
[edit interfaces]
user@host#set apfe0 anchoring-options primary-list pfe-7/0/0
user@host#set apfe0 anchoring-options primary-list pfe-8/0/0
user@host#set apfe0 anchoring-options secondary pfe-9/0/0 warm-standby
user@host#set apfe0 anchoring-options warm-standby
```

**Results** From configuration mode, confirm your configuration by entering the **show interfaces** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, this **show** command output includes only the configuration statements that are relevant to this example.

```
ams0 {
  load-balancing-options {
    member-interface mams-4/1/0;
    member-interface mams-5/1/0;
    member-failure-options {
      redistribute-all-traffic {
        enable-rejoin;
      }
    }
    high-availability-options {
      many-to-one {
        preferred-backup mams-5/1/0;
      }
    }
  }
  unit 1 {
    family inet;
  }
  unit 2 {
    family inet;
  }
}
ams1 {
  load-balancing-options {
    member-interface mams-4/0/0;
    member-interface mams-5/0/0;
    high-availability-options {
      many-to-one {
        preferred-backup mams-5/0/0;
      }
    }
  }
  unit 1 {
    family inet;
  }
  unit 2 {
    family inet;
  }
}

apfe0 {
```

```
anchoring-options {  
  primary-list {  
    pfe-7/0/0;  
    pfe-8/0/0;  
  }  
  secondary pfe-9/0/0;  
  warm-standby;  
}
```

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

### Verifying Redundancy

---

**Purpose** Verify that redundancy is enabled or not.

**Action** From operational mode, enter the **show unified-edge ggsn-pgw interfaces redundancy** command.



.....  
**NOTE:** To view failover statistics, enter the **show unified-edge ggsn-pgw exception-handling statistics failover** command.  
.....

**Meaning** The output shows the redundancy parameters or failover statistics configured on the gateway

**Related Documentation**

- [Broadband Gateway Redundancy Overview on page 78](#)
- [Configuring Session DPC Redundancy on page 80](#)
- [Configuring Interface Redundancy on page 82](#)
- [Configuring Anchor Session DPCs and PFEs on page 75](#)
- *interfaces (Aggregated Multiservices)*
- *interfaces (Aggregated Packet Forwarding Engine)*
- [Understanding the Broadband Gateway Anchor Failover Behavior on page 84](#)



## CHAPTER 6

# Configuring IP Reassembly

- [IP Packet Fragment Reassembly for Mobility Overview on page 91](#)
- [Understanding Default IP Fragment Handling on page 94](#)
- [Configuring IP Inline Reassembly for Mobility on page 96](#)
- [Configuring Software-Based Fragment Reassembly Parameters on page 98](#)
- [Example: Configuring Inline IP Packet Fragment Reassembly on page 99](#)
- [Example: Configuring Software-Based IP Reassembly Parameters on page 107](#)

### IP Packet Fragment Reassembly for Mobility Overview

---

You can configure the MobileNext Broadband Gateway so that reassembly of fragmented IP packets is carried out inline (on the Packet Forwarding Engine) instead of performing IP reassembly on the services PIC. By default, IP reassembly is carried out on the services PIC. You can change the default behavior of the gateway; whether the gateway is configured as a Serving Gateway (S-GW), Packet Data Network Gateway (P-GW), or Gateway GPRS Support Node (GGSN). Although Serving Gateway Support Nodes (SGSNs) also reassemble IP packets, the broadband gateway cannot be configured as an SGSN.

Fragmentation of IP packets for transmission and the need to reassemble the IP packets at a destination is a feature of how Layer 2 (the frame layer) and Layer 3 (the packet layer) operate. That is, the maximum size of a frame, set by the Maximum Transmission Unit (MTU) value, and the maximum size of a packet are determined independently. It is usually the case that the packet size can far exceed the MTU size. If the packet size (data plus IP and other headers) exceeds the allowable frame size (usually set by the transport medium limits), the packet must be fragmented at the sender and split across multiple frames for transmission. Frames are always processed immediately, as they arrive (if error-free), but packet fragments cannot be processed until the whole packet has been reassembled. Each packet fragment inside a frame series, except the last, has the more fragments (MF) IP header bit set, indicating that this packet is part of a whole. The last packet fragment inside a frame does not have the MF bit set and therefore ends the fragment sequence. Once all of the fragments of a packet have arrived, the entire packet is reassembled.

When memory buffers for networking were limited, heavy intervals of arriving fragmented traffic easily resulted in performance degradations or even complete “reassembly deadlock,” with buffers occupied only with fragments and no room for any arriving

fragment that might complete a packet. In some cases, a packet fragment was discarded only to find that the newly arrived frame would have completed the packet just thrown away. It is clear that efficient reassembly is important for network throughput, scalability, and graceful response to congestion.

In some cases, you can avoid the need to fragment packets on a mobile network by adjusting the MTU size to account for added headers such as GTP. However, in cases where multiple vendors are used or organization lines are crossed, this MTU adjustment might not be possible and IP fragmentation is unavoidable.

**Figure 31: Fragmented Packet Requiring Reassembly**

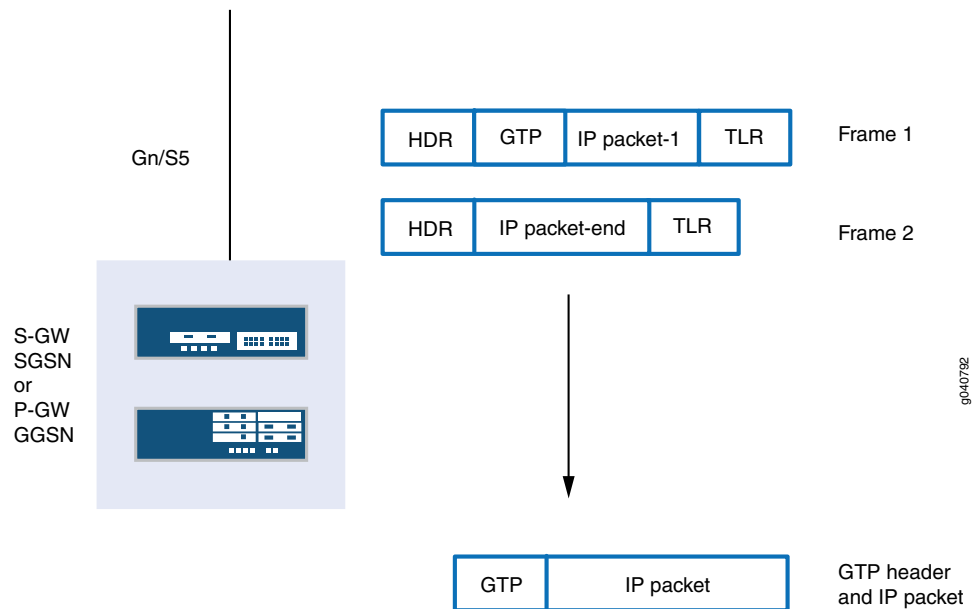
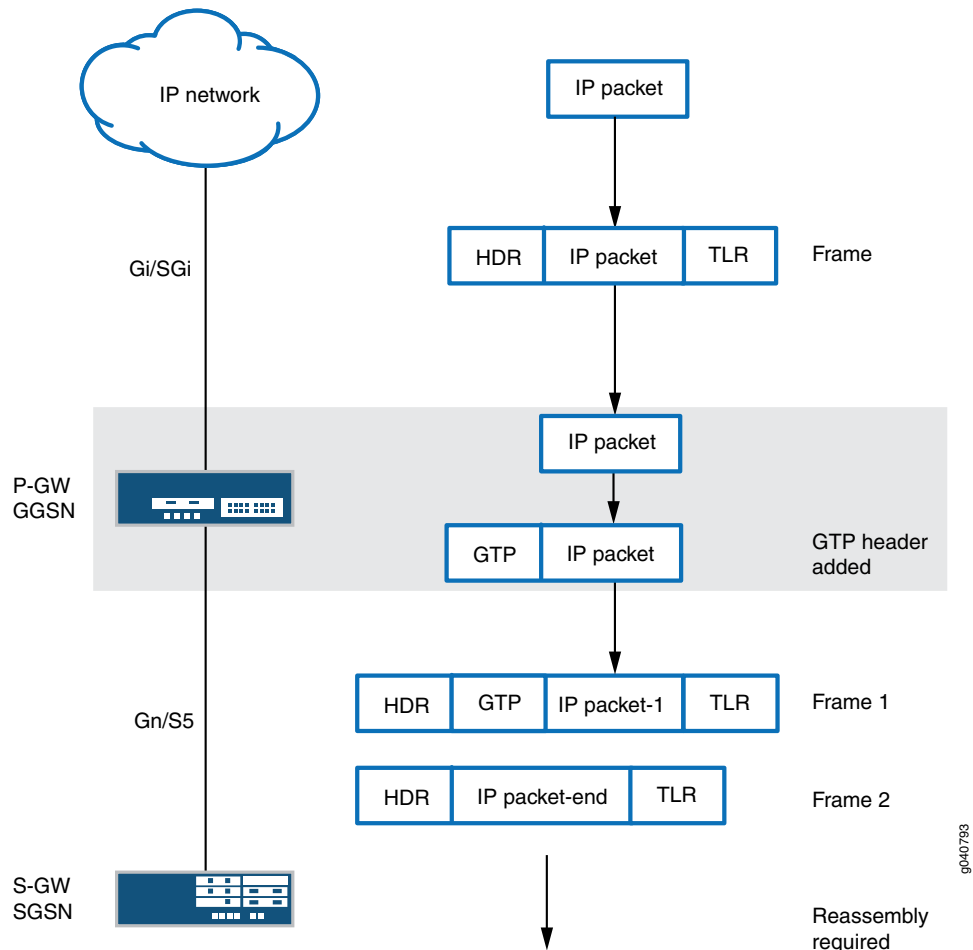


Figure 31 on page 92 shows a fragmented packet containing user data that requires reassembly on arrival on the Gn or S5 interface. On the broadband gateway, by default, IP reassembly is carried out using software on the services PIC. You can configure the broadband gateway to perform IP reassembly of fragmented IP packets inline, on the Packet Forwarding Engine, instead of software default reassembly on the services PIC. However, inline reassembly requires the dedication of Packet Forwarding Engine resources for reassembly, which means these resources cannot be used for their usual purposes. You should consider potential trade-offs before changing the default behavior of the gateway.

As shown in Figure 32 on page 93, a framed downstream packet from an IP network to a mobile device is sent over a Gi (3G) or SGi (LTE) interface to a GGSN or P-GW. At the GGSN/P-GW, the frame is processed and a 20-byte GTP-U header is added to the packet. If the packets use the most common MTU size of 1500 bytes (for network efficiency), the added 20 bytes put the data unit over the allowable 1500-byte limit ( $1500 + 20 = 1520$ ). To send the 1520-byte packet over the Gn (3G) or S5 (LTE) interface to the SSGN or S-GW, the GGSN or P-GW must fragment the packet and distribute the 1520 bytes into two frames (1500 bytes and 20 bytes). Because frames are processed immediately as they arrive (there is no such thing as "frame 1 of 2"), the first packet fragment must be

kept until the second frame is processed and completes the packet. Then the whole packet with GTP-U header can be processed, routed, and sent on downstream. This requires the SSGN or S-GW to perform the reassembly of the IP packet. Heavy traffic loads create an environment that forces the receiving node to keep track of and process many fragments at the same time.

Figure 32: A GTP-U Header Causing Fragmentation



Inline IP reassembly is enabled at the gateway level (for example, the entire P-GW or S-GW). Fragments for all IP addresses associated with the broadband gateway configured for inline reassembly are stored on the same line card as they arrive or redirected to a line card dedicated to inline reassembly based on configuration. The mobility line cards reserve 2 MB of memory for storing fragments (non-mobility line cards reserve 8 MB). When there are multiple line cards performing reassembly, the fragments are load-balanced based on a hash of the fragment's IP source address, IP identifier, and the relevant Virtual Routing and Forwarding table (VRF).

You have two options when configuring inline IP reassembly:

- Using the single **ip-reassembly** statement. However, this option does not reassemble IP fragments arriving on different Packet Forwarding Engines.

- Using a service set and related statements. This option reassembles IP fragments arriving on different Packet Forwarding Engines correctly.



**NOTE:** If you configure *single statement* IP fragment reassembly with the `ip-reassembly` statement, then the broadband gateway does not reassemble fragments arriving on different Packet Forwarding Engines correctly. These IP fragments are stored, but cannot be reassembled and eventually time out and are dropped. The inline reassembly timeout parameter is 20 milliseconds (ms) and cannot be changed. The timeout values from 2 (default) through 60 seconds are set for an IP reassembly profile at the `[edit services ip-reassembly ip-reassembly-profile-name inline-services]` hierarchy level and apply to IP reassembly on the services PIC only.

Inline IP reassembly does not preclude the use of the services PIC. The Packet Forwarding Engine could run out of memory to store fragments. In that case, new fragments that arrive are directed to the services PIC (if available) as a kind of “backup.” Once the Packet Forwarding Engine memory usage recovers, all fragments are again processed inline in the Packet Forwarding Engine. Inline reassembly enhances the performance of the broadband gateway.

It should be noted that other scenarios involve IP fragment reassembly. For instance, IPsec is often used to encapsulate GTP packets on the S1-U interfaces from eNodeB to S-GW. IPsec encapsulation often causes packet fragmentation as well.

**Related  
Documentation**

- [Configuring IP Inline Reassembly for Mobility on page 96](#)
- [Example: Configuring Inline IP Packet Fragment Reassembly on page 99](#)

---

## Understanding Default IP Fragment Handling

The MobileNext Broadband Gateway handles IP packet fragments differently than packets containing a single segment or datagram.

It is most efficient to process GPRS tunneling protocol (GTP) and IP packets immediately, as they arrive at the broadband gateway. Typically, a hardware data path is used to transfer packets to and from the anchor session Dense Port Concentrator (DPC) (for the control plane) or the interface Packet Forwarding Engine (for the data plane). However, fragmented packets require complete reassembly before processing can begin, because upper layer (Layer 4 and above) information will be missing in all but the first fragment. By default, the broadband gateway uses software on the services PIC to reassemble the fragment. You can control many of the parameters associated with the software-based fragment reassembly process.

You can configure the time interval that the anchor session DPCs wait for fragments to arrive. You can also configure the maximum number of packets that can be waiting for fragments. Both of these methods prevent the session DPCs from waiting for fragments that might never arrive.

Fragments arriving on the interface are load-balanced based on a hash of the fragment's IP source address, IP identifier, and the relevant Virtual Routing and Forwarding table (VRF) across the list of services PICs configured for that gateway.

- Gateway-1, a Packet Data Network Gateway (P-GW), has PICs 1, 3, and 4. Fragments for Gateway-1 are load-balanced across PICs 1, 3, and 4.
- Gateway-2, a Serving Gateway (S-GW), has PICs 2 and 5. Fragments for Gateway-2 are load-balanced across PICs 2 and 5.

**Related  
Documentation**

- [Configuring Software-Based Fragment Reassembly Parameters on page 98](#)
- [Configuring GGSN or P-GW Software Data Path Traceoptions on page 55](#)
- [Configuring S-GW Software Data Path Traceoptions on page 62](#)
- [Example: Configuring Inline IP Packet Fragment Reassembly on page 99](#)
- [Understanding the Broadband Gateway Software Data Path on page 10](#)
- [Example: Configuring Software-Based IP Reassembly Parameters on page 107](#)

## Configuring IP Inline Reassembly for Mobility

---

This procedure shows how to configure the MobileNext Broadband Gateway so that reassembly of fragmented IP packets is carried out inline (on the Packet Forwarding Engine) instead of performing IP reassembly using software on the services PIC. By default, IP reassembly is carried out on the services PIC. This example changes the default behavior of the gateway; whether the gateway is configured as a Serving Gateway (S-GW), Packet Data Network Gateway (P-GW), or Gateway GPRS Support Node (GGSN). Although Serving Gateway Support Nodes (SGSNs) also reassemble IP packets, the broadband gateway cannot be configured as an SGSN.

You can either configure inline IP reassembly for a broadband gateway as a single statement (**set unified-edge gateways ggsn-pgw gateway-name inline services ip-reassembly** or **set unified-edge gateways sgw gateway-name inline services ip-reassembly**), or as part of a service set. This example configures service set inline reassembly, which handles fragments properly even when they arrive on different Packet Forwarding Engines.



**NOTE:** If you configure *single statement* IP fragment reassembly with the **ip-reassembly** statement, then the broadband gateway does not reassemble fragments arriving on different Packet Forwarding Engines correctly. These IP fragments are stored, but cannot be reassembled and eventually time out and are dropped. The inline reassembly timeout parameter is 20 milliseconds (ms) and cannot be changed. The timeout values from 2 (default) through 60 seconds are set for an IP reassembly profile at the [edit services ip-reassembly *ip-reassembly-profile-name* inline-services] hierarchy level and apply to IP reassembly on the services PIC only.

Before you configure inline IP reassembly, be sure you have:

- Configured the broadband gateway correctly.
- Configured a valid MTU size and GTP-U parameters.

To configure inline IP reassembly:

1. Configure the chassis-level bandwidth used by the inline services (si-) interface on the FPC and PIC slot for inline IP fragment reassembly.

```
[edit chassis]
user@host# set fpc 2 pic 1 inline-services bandwidth 10g
```



**NOTE:** This configuration is not unique to mobility.

2. Configure the interface-level logical unit used by the inline services (si-) interface on the FPC and PIC slot for inline IP fragment reassembly.

```
[edit interfaces]
user@host# set si-2/1/0 unit 0 family inet
```

```
user@host# set si-2/1/0 unit 0 service-domain inside
```



**NOTE:** This configuration is not unique to mobility. However, you must configure the family (inet) and service domain (inside) as shown.

3. Configure the IP reassembly rule (**ip-reassembly-rule-1**) for IP reassembly in the **input** match direction.

```
[edit services]
```

```
user@host# set ip-reassembly-rules rule ip-reassembly-rule-1 match-direction input
```

4. Configure the service set (**ip-reassembly-set**) for the IP reassembly rule in the input match direction (the **local** option loops the reassembled packets back to the local interface).

```
[edit services]
```

```
user@host# set service-set ip-reassembly-set ip-reassembly-rules ip-reassembly-rule-1
```

```
user@host# set service-set ip-reassembly-set next-hop-service inside-service-interface  
si-2/1/0.0
```

```
user@host# set service-set ip-reassembly-set next-hop-service  
outside-service-interface-type local
```



**NOTE:** You must configure both inside (si- interface) and outside type (local) service interfaces statements. This **next-hop-service** configuration is not unique to mobility. However, the **ip-reassembly-rules** statements are unique to mobility.

5. Configure the service set (**ip-reassembly-set**) for IP reassembly to bind to the broadband gateway at the **[edit unified-edge gateways]** hierarchy level.

```
[edit unified-edge gateways ggsn-pgw MBG-PGW-1]
```

```
[edit unified-edge gateways sgw MBG-SGW-2]
```

```
user@host# set inline-services ip-reassembly service-set ip-reassembly-set
```

#### Related Documentation

- [IP Packet Fragment Reassembly for Mobility Overview on page 91](#)
- [Understanding Default IP Fragment Handling on page 94](#)
- [Configuring GGSN or P-GW Software Data Path Traceoptions on page 55](#)
- [Configuring S-GW Software Data Path Traceoptions on page 62](#)
- [Example: Configuring Inline IP Packet Fragment Reassembly on page 99](#)
- [Example: Configuring Software-Based IP Reassembly Parameters on page 107](#)

## Configuring Software-Based Fragment Reassembly Parameters

---

By default, on the MobileNext Broadband Gateway, anchor session Dense Port Concentrators (DPCs) reassemble arriving user plane packet fragments in order to have complete Layer 4 and above information. To prevent reassembly deadlock while waiting for fragments that never arrive, you can configure the time interval that the anchor session DPCs wait for fragments to arrive and the maximum number of packets that can be waiting for fragments.

Before you begin configuring reassembly parameters on the broadband gateway, you should have done the following:

- Configured the chassis of the broadband gateway
- Configured the interfaces of the broadband gateway
- Configured the general redundancy parameters for the broadband gateway

To determine the software-based fragment reassembly behavior, you configure the timeout and maximum packets pending fragment parameters. You can group these parameters into an IP reassembly profile. More than one IP reassembly profile can be configured and applied to a particular gateway.

To configure the reassembly parameters:

1. Configure a value for the **timeout** in the reassembly profile.

```
[edit services ip-reassembly profile reassembly-profile-one ]
user@host# set timeout 4
```



**NOTE:** You can set the timeout value from 2 through 60 seconds. The default value is 4 seconds.

2. Configure a value for the **max-reassembly-pending-packets** in the reassembly profile.

```
[edit services ip-reassembly profile reassembly-profile-one ]
user@host# set max-reassembly-pending-packets 1000
```



**NOTE:** You can set the maximum packets pending reassembly value from 100 through 100,000 packets. The default value is 1000 packets.

3. Configure the broadband gateway to use the IP reassembly profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 ]
user@host# set ip-reassembly-profile reassembly-profile-one
```



**NOTE:** You can configure multiple IP reassembly profiles, but apply only one to a particular broadband gateway. You can also apply the profile to an S-GW configuration.



**Related Documentation**

- [IP Packet Fragment Reassembly for Mobility Overview on page 91](#)
- [Understanding Default IP Fragment Handling on page 94](#)
- [Configuring GGSN or P-GW Software Data Path Traceoptions on page 55](#)
- [Configuring S-GW Software Data Path Traceoptions on page 62](#)
- [Example: Configuring Inline IP Packet Fragment Reassembly on page 99](#)
- [Example: Configuring Software-Based IP Reassembly Parameters on page 107](#)

---

## Example: Configuring Inline IP Packet Fragment Reassembly

This example shows how to configure the MobileNext Broadband Gateway so that reassembly of fragmented IP packets is carried out inline (on the Packet Forwarding Engine) instead of performing IP reassembly on the services PIC. By default, IP reassembly is carried out on the services PIC. This example changes the default behavior of the gateway; whether the gateway is configured as a Serving Gateway (S-GW), Packet Data Network Gateway (P-GW), or Gateway GPRS Support Node (GGSN). Although Serving Gateway Support Nodes (SGSNs) also reassemble IP packets, the broadband gateway cannot be configured as an SGSN.

- [Requirements on page 99](#)
- [Overview on page 99](#)
- [Configuration on page 103](#)
- [Verification on page 106](#)
- [Troubleshooting on page 107](#)

### Requirements

This example uses the following hardware and software components:

- A supported MX Series chassis configured with supported line cards and a services PIC.
- A supported and properly installed version of 64-bit Junos OS and the **jmobile** software package.
- Correct configuration as a P-GW, S-GW, or GGSN with corresponding interfaces.

Before you configure inline IP reassembly, be sure you have:

- Configured the broadband gateway correctly.
- Configured a valid MTU size and GTP-U parameters.

### Overview

Fragmentation of IP packets for transmission and the need to reassemble the IP packets at a destination is a feature of how Layer 2 (the frame layer) and Layer 3 (the packet layer) operate. That is, the maximum size of a frame, set by the Maximum Transmission

Unit (MTU) value, and the maximum size of a packet are determined independently. It is usually the case that the packet size can far exceed the MTU size. If the packet size (data plus IP and other headers) exceeds the allowable frame size (usually set by the transport medium limits), the packet must be fragmented at the sender and split across multiple frames for transmission. Frames are always processed immediately, as they arrive (if error-free), but packet fragments cannot be processed until the whole packet has been reassembled. Each packet fragment inside a frame series, except the last, has the more fragments (MF) IP header bit set, indicating that this packet is part of a whole. The last packet fragment inside a frame does not have the MF bit set and therefore ends the fragment sequence. Once all of the fragments of a packet have arrived, the entire packet are reassembled.

When memory buffers for networking were limited, heavy intervals of arriving fragmented traffic easily resulted in performance degradations or even complete “reassembly deadlock,” with buffers occupied only with fragments and no room for any arriving fragment that might complete a packet. In some cases, a packet fragment was discarded only to find that the newly arrived frame would have completed the packet just thrown away. It is clear that efficient reassembly is important for network throughput, scalability, and graceful response to congestion.

In some cases, you can avoid the need to fragment packets on a mobile network by adjusting the MTU size to account for added headers such as GTP. However, in cases where multiple vendors are used or organization lines are crossed, this MTU adjustment might not be possible and IP fragmentation is unavoidable.

**Figure 33: Fragmented Packet Requiring Reassembly**

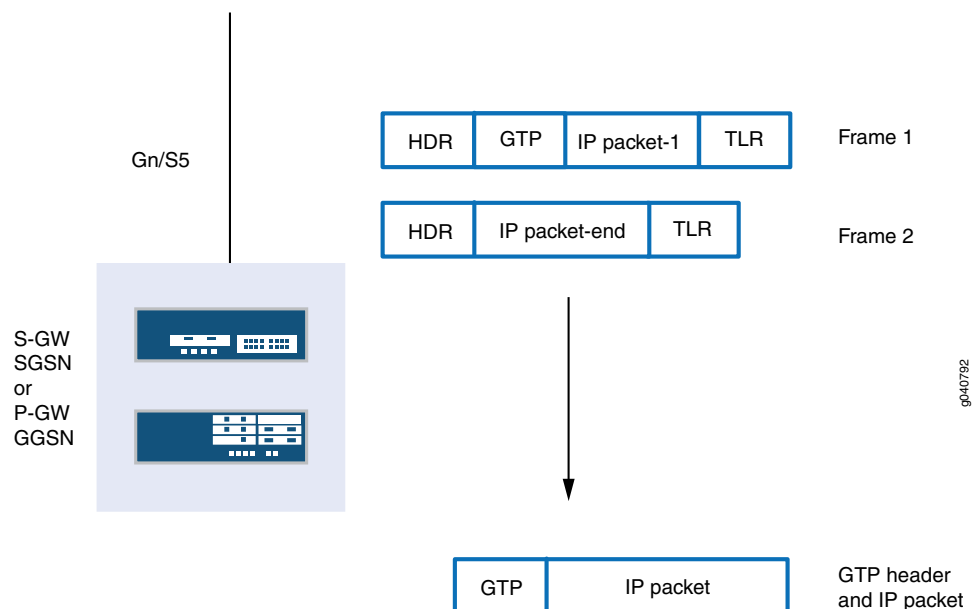


Figure 33 on page 100 shows a fragmented packet containing user data that requires reassembly on arrival on the Gn or S5 interface. On the broadband gateway, IP reassembly is carried out on the services PIC by default. This example configures the broadband gateway to perform IP reassembly of fragmented IP packets inline, on the Packet

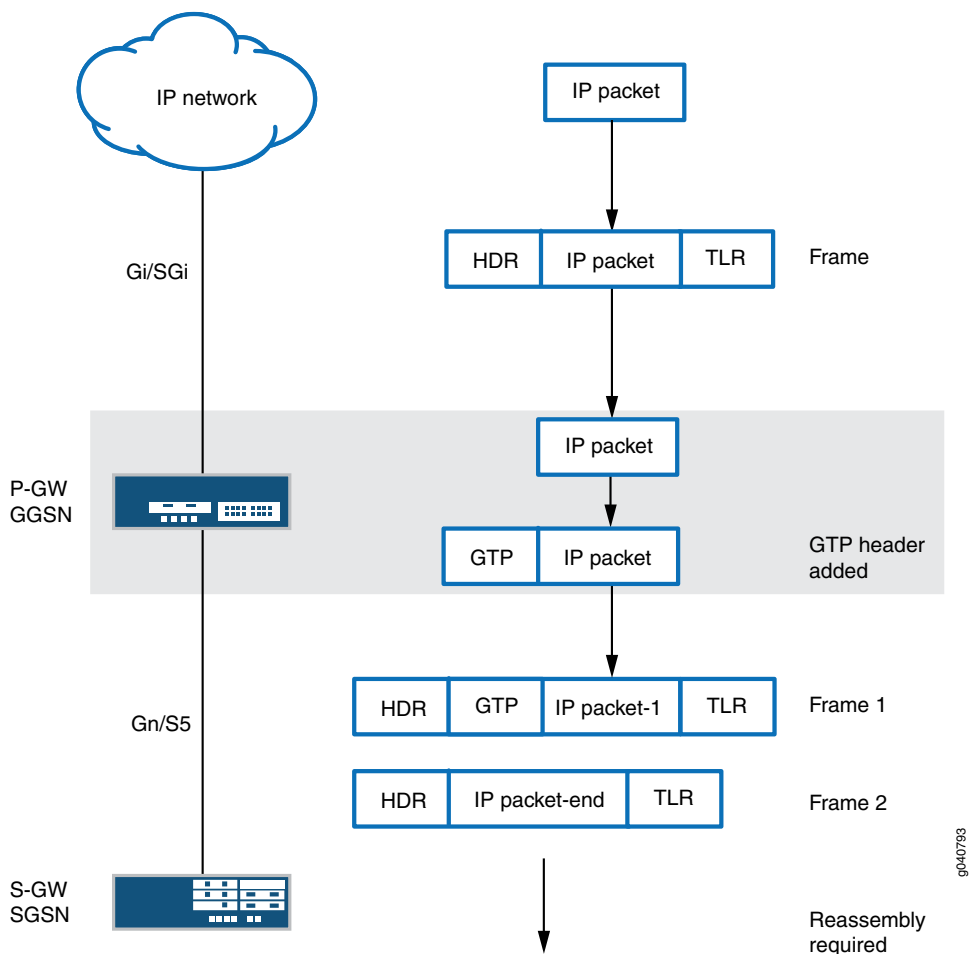
Forwarding Engine. However, inline reassembly requires the dedication of Packet Forwarding Engine resources for reassembly, which means these resources cannot be used for their usual purposes. You should consider potential trade-offs before changing the default behavior of the gateway.

### Topology

---

The topology for this inline reassembly example consists of two mobile network nodes, the interfaces connecting them to each other, and an IP network such as the Internet. As shown in [Figure 34 on page 102](#), a framed downstream packet from an IP network to mobile device is sent over a Gi (3G) or SGi (LTE) interface to a GGSN or P-GW. At the GGSN/P-GW, the frame is processed and a 20-byte GTP-U header is added to the packet. If the packets use the most common MTU size of 1500 bytes (for network efficiency), the added 20 bytes put the data unit over the allowable 1500-byte limit ( $1500 + 20 = 1520$ ). To send the 1520-byte packet over the Gn (3G) or S5 (LTE) interface to the SSGN or S-GW, the GGSN or P-GW must fragment the packet and distribute the 1520 bytes into two frames (1500 bytes and 20 bytes). Because frames are processed immediately as they arrive (there is no such thing as “frame 1 of 2”), the first packet fragment must be kept until the second frame is processed and completes the packet. Then the whole packet with GTP-U header can be processed, routed, and sent on downstream. This requires the SSGN or S-GW to perform the reassembly of the IP packet. Heavy traffic loads create an environment that forces the receiving node to keep track of and process many fragments at the same time.

Figure 34: A GTP-U Header Causing Fragmentation



Inline IP reassembly is enabled at the gateway level (for example, the entire P-GW or S-GW). Fragments for all IP addresses associated with the broadband gateway configured for inline reassembly are stored on the same line card as they arrive or redirected to a line card dedicated to inline reassembly based on configuration. The mobility line cards reserve 2 MB of memory for storing fragments (non-mobility line cards reserve 8 MB). When there are multiple line cards performing reassembly, the fragments are load-balanced based on a hash of the fragment's IP source address, IP identifier, and the relevant Virtual Routing and Forwarding table (VRF).



**NOTE:** If you configure *single statement* IP fragment reassembly with the `ip-reassembly` statement, then the broadband gateway does not reassemble fragments arriving on different Packet Forwarding Engines correctly. These IP fragments are stored, but cannot be reassembled and eventually time out and are dropped. The inline reassembly timeout parameter is 20 milliseconds (ms) and cannot be changed. The timeout values from 2 (default) through 60 seconds are set for an IP reassembly profile at the [edit services ip-reassembly *ip-reassembly-profile-name* inline-services] hierarchy level and apply to IP reassembly on the services PIC only.

Inline IP reassembly does not preclude the use of the services PIC. The Packet Forwarding Engine could run out of memory to store fragments. In that case, new fragments that arrive are directed to the services PIC (if available) as a kind of “backup.” Once the Packet Forwarding Engine memory usage recovers, all fragments are again processed inline in the Packet Forwarding Engine.

It should be noted that other topologies could have been used for this example. For instance, IPsec is often used to encapsulate GTP packets on the S1-U interfaces from eNodeB to S-GW. IPsec encapsulation often causes packet fragmentation as well.

## Configuration

To configure inline IP reassembly on a Service Gateway (S-GW), perform these tasks:

- [Configuring Inline IP Reassembly on page 103](#)
- [Results on page 105](#)

### CLI Quick Configuration

```
set chassis fpc 2 pic 1 inline-services bandwidth 10g
set interfaces si-2/1/0 unit 0 family inet
set interfaces si-2/1/0 unit 0 service-domain inside
set services ip-reassembly-rules ip-reassembly-rule-1
set services service-set ip-reassembly-set rule ip-reassembly-rules ip-reassembly-rule-1
set services service-set ip-reassembly-set next-hop-service inside-service-interface
  si-2/1/0.0
set services service-set ip-reassembly-set next-hop-service outside-service-interface-type
  local
set unified-edge gateways sgw SGW1 inline-services ip-reassembly service-set
  ip-reassembly-set
```



**NOTE:** You can also configure inline IP reassembly on a GGSN or P-GW.

## Configuring Inline IP Reassembly

### Step-by-Step Procedure

To configure inline IP reassembly:

1. Configure the chassis-level bandwidth used by the inline services (`si-`) interface on the FPC and PIC slot for inline IP fragment reassembly.  
[edit chassis]

```
user@host# set fpc 2 pic 1 inline-services bandwidth 10g
```



**NOTE:** This configuration is not unique to mobility.

2. Configure the interface-level logical unit used by the inline services (**si-**) interface on the FPC and PIC slot for inline IP fragment reassembly.

```
[edit interfaces]
```

```
user@host# set si-2/1/0 unit 0 family inet
```

```
user@host# set si-2/1/0 unit 0 service-domain inside
```



**NOTE:** This configuration is not unique to mobility. However, you must configure the family (**inet**) and service domain (**inside**) as shown.

3. Configure the IP reassembly rule (**ip-reassembly-rule-1**) for IP reassembly in the **input** match direction.

```
[edit services]
```

```
user@host# set ip-reassembly-rules rule ip-reassembly-rule-1 match-direction input
```

4. Configure the service set (**ip-reassembly-set**) for IP reassembly in the input match direction (the **local** option loops the reassembled packets back to the local interface).

```
[edit services]
```

```
user@host# set service-set ip-reassembly-set reassembly-rules ip-reassembly-rule
```

```
user@host# set service-set ip-reassembly-set next-hop-service
```

```
inside-service-interface si-2/1/0.0
```

```
user@host# set service-set ip-reassembly-set next-hop-service
```

```
outside-service-interface-type local
```



**NOTE:** You must configure both inside (**si-** interface) and outside type (**local**) service interfaces statements. This **next-hop-service** configuration is not unique to mobility. However, the **reassembly-rules** statements are unique to mobility. The reassembly rule is not formulated outside of the service set: this statement simply initiates the reassembly process.

5. Configure the service set (**ip-reassembly-set**) for IP reassembly to bind to the broadband gateway at the **[edit unified-edge gateways sgw MBG-SGW-2]** hierarchy level.

```
[edit unified-edge gateways sgw MBG-SGW-2]
```

```
user@host# set inline-services ip-reassembly service-set ip-reassembly-set
```

## Results

From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, these **show** command outputs include only the configuration that is relevant to this example.

```
[edit chassis]
fpc 2 {
  pic 1 {
    inline-services {
      bandwidth 10g;
    }
  }
}

[edit interfaces]
si-2/1/0 {
  unit 0 {
    family inet;
    service-domain inside;
  }
}

[edit services]
ip-reassembly {
  rule ip-reassembly-rule-1 {
    match-direction input;
  }
}
service-set ip-reassembly-set {
  reassembly-rules {
    ip-reassembly-rule;
  }
  next-hop-service {
    inside-service-interface si-2/1/0.0;
    outside-service-interface-type local;
  }
}

[edit unified-edge gateways sgw MBG-SGW-2]
inline-services {
  ip-reassembly service-set ip-reassembly-set;
}
```

## Verification

### Verifying Inline IP Reassembly Configuration

**Purpose** Verify that the Packet Forwarding Engine of the Gn or S5 or S8 interfaces associated with the broadband gateway where fragments are arriving have non-zero fragment counters for the interfaces and the interfaces have successfully reassembled packets.

**Action** From operational mode, enter the **show services inline ip-reassembly statistics** command.

```
user@SGW-2# show services inline ip-reassembly statistics
FPC: 2
```

```
=====
```

	Total	Current Rate
Total Fragments Received	1004681374	6213217
First Fragments	502335971	3106615
Intermediate Fragments	0	0
Last Fragments	502345403	3106602
Total Packets Successfully Reassembled	71135257	432439
Approximate Packets Pending Reassembly	2408	
Fragments Dropped Reasons	1404714	7700
Buffers not available	0	0
Fragments per packet exceeded	0	0
Packet length exceeded	0	0
Record insert error	0	0
Record in use error	1404714	7700
Duplicate first fragments	0	0
Duplicate last fragments	0	0
Missing first fragment	0	0
Reassembly Errors Reasons	0	0
Fragment not found	0	0
Fragment not in sequence	0	0
ASIC errors	0	0
Aged out packets	6147008	37279
Total Fragments Successfully Reassembled	142270514	864878
Total Fragments Dropped	7551722	44979
Buffers not available	0	0
Fragments per packet exceeded	0	0
Packet length exceeded	0	0
Record insert error	0	0
Record in use error	1404714	7700
Duplicate first fragments	0	0
Duplicate last fragments	0	0
Missing first fragment	0	0
Fragment not found	0	0
Fragment not in sequence	0	0
ASIC errors	0	0
Aged out fragments	6147008	37279
Total fragments punted to UPIC	854858289	5303865



**Meaning** The output associated with FPC 2 (in this case) displays non-zero values for packet fragments and successfully reassembled packets. Errors and dropped fragments are minimal.

## Troubleshooting

To troubleshoot inline IP reassembly, perform these tasks:

- [Troubleshooting Non-Incrementing Counters on page 107](#)
- [Troubleshooting Zero Successfully Reassembled Packets on page 107](#)

---

### Troubleshooting Non-Incrementing Counters

**Problem** The total fragment received counter and current rate fields are not incrementing.

**Solution** There are no fragments arriving for the gateway, or the inline reassembly statement is set for the wrong gateway.

---

### Troubleshooting Zero Successfully Reassembled Packets

**Problem** The counters show zero value for successfully reassembled packets.

**Solution** Examine the reasons for fragment errors and dropped fragments in the **show services inline ip-reassembly statistics** command output. This is usually sufficient to determine the solution to the issue.

**Related Documentation**

- [IP Packet Fragment Reassembly for Mobility Overview on page 91](#)
- [Configuring IP Inline Reassembly for Mobility on page 96](#)
- [Example: Configuring Software-Based IP Reassembly Parameters on page 107](#)

---

## Example: Configuring Software-Based IP Reassembly Parameters

This example shows how to configure software-based IP reassembly parameters on the MobileNext Broadband Gateway. A software-based IP reassembly profile is configured.

- [Requirements on page 107](#)
- [Overview on page 108](#)
- [Configuration on page 108](#)
- [Verification on page 109](#)

## Requirements

This example uses the following hardware and software components:

- An MX Series chassis equipped with session Dense Port Concentrators (DPCs) and three interface Packet Forwarding Engines (housed in DPCs or Modular Port Concentrators [MPCs]).

- Junos OS Mobility package

Before you begin:

- Install the chassis hardware.
- Configure the chassis, as well as interfaces, anchors, and (optionally) redundancy.

## Overview

There are four exceptions to the general rule that user packets flow only through interface Packet Forwarding Engine hardware:

- Anchor Packet Forwarding Engine failovers (N:1)
- Reassembly of GPRS tunneling protocol, user plane (GTP-U), and mobility control plane (for instance, authentication, authorization, and accounting [AAA]) fragments
- IPv6 router advertisements and router solicitation packet handling
- GTP-U error indication generation

The first and last items have no configurable parameters. This example configures parameters for software-based IP fragment reassembly (inline IP reassembly is covered elsewhere). The software-based IP fragment reassembly parameters are configured in **reassembly-profile-one** (you can have multiple reassembly profiles) and applied to the gateway (**MBG1**). All of the statements in this example use the default values.



**NOTE:** Inline IP reassembly configuration, as opposed to the default mode, is covered in other topics.

## Configuration

### CLI Quick Configuration

The parameters for software-based IP fragment reassembly are configured by:

```
[edit services ip-reassembly profile reassembly-profile-one]
set timeout 4 # The default (seconds)
set max-reassembly-pending-packets 1000 # The default
```

```
[edit unified-edge gateways ggsn-pgw MBG1]
set ip-reassembly reassembly-profile-one # You can apply only one profile to a gateway
```

**Results** From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, these **show** command outputs include only the configuration that is relevant to this example.

```
show services ip-reassembly reassembly-profile-one
timeout 2;
max-reassembly-pending-packets 100;
```

```
show unified-edge gateways ggsn-pgw MBG1
ip-reassembly-profile {
  reassembly-profile-one;
}
```

After you configure the device, enter **commit** from configuration mode.

## Verification

### Verifying the Software-Based IP Reassembly Configuration

<b>Purpose</b>	Verify that software-based IP reassembly data path handling is operating.
<b>Action</b>	From operational mode, enter the <b>show unified-edge gateways ggsn-pgw ip-reassembly statistics</b> command.
<b>Meaning</b>	Non-zero values indicate that reassembly is functioning.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">IP Packet Fragment Reassembly for Mobility Overview on page 91</a></li><li>• <a href="#">Configuring IP Inline Reassembly for Mobility on page 96</a></li><li>• <a href="#">Example: Configuring Inline IP Packet Fragment Reassembly on page 99</a></li><li>• <a href="#">Understanding Default IP Fragment Handling on page 94</a></li><li>• <a href="#">Configuring Software-Based Fragment Reassembly Parameters on page 98</a></li><li>• <a href="#">Configuring GGSN or P-GW Software Data Path Traceoptions on page 55</a></li><li>• <a href="#">Configuring S-GW Software Data Path Traceoptions on page 62</a></li></ul>



## PART 3

# APN Configuration

- [Configuring APNs on page 113](#)



## CHAPTER 7

# Configuring APNs

- [Configuring APNs on the MobileNext Broadband Gateway Overview on page 113](#)
- [User-Session Routing Overview on page 115](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 117](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 121](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 122](#)
- [Configuring Charging, Local Policy, and Policy and Charging Enforcement Function Profiles on a Broadband Gateway APN on page 131](#)
- [Configuring Mobile Interfaces for APNs on page 133](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 134](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 135](#)
- [Configuring User Options on a Broadband Gateway APN on page 141](#)
- [Example: Configuring Broadband Gateway APNs on page 143](#)
- [Networks Behind the Mobile Device Overview on page 146](#)
- [Configuring the Networks Behind the Mobile Equipment Feature on page 148](#)
- [Example: Configuring the Networks Behind the Mobile Device Feature on page 150](#)
- [HTTP Header Enrichment Overview on page 153](#)
- [Configuring HTTP Header Enrichment on page 154](#)
- [Example: Configuring HTTP Header Enrichment on page 157](#)

### Configuring APNs on the MobileNext Broadband Gateway Overview

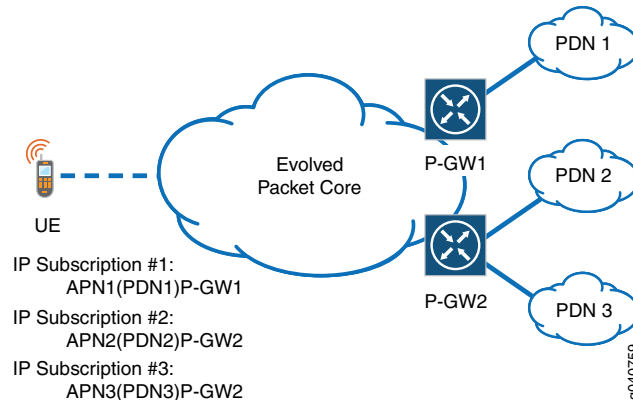
---

You configure an access point name (APN) on the MobileNext Broadband Gateway to contain the parameters that characterize the user session to an IP network. The APN determines authorization and address allocation methods, charging rules, several types of timeouts, and various other parameters.

The broadband gateway requires more than the typical provider edge (PE) router configuration to function in a mobile network and allow mobile devices to access the Internet or a private IP network. The broadband gateway uses a unique identifier to identify each attached IP network, which is called an APN network or Packet Data Network (PDN). An APN should be as stable as the IP network it represents. The broadband gateway uses various rules, called the APN service selection method, to determine which

APN and service types a Mobile Station (MS) or user equipment device should use. Mobile devices can subscribe to multiple PDNs and services, which can be accessed through different broadband gateways. [Figure 35 on page 114](#) shows the relationship between APNs and broadband gateways in a 4G network.

**Figure 35: APNs and P-GWs in the 4G Architecture**



The parameters you configure for an APN on the broadband gateway fall into five categories:

- General APN parameters:
  - Interface
  - Servers
  - Timers
  - Miscellaneous parameters
- Restriction value
- User options
- Address assignment
- Anchor PIC or Packet Forwarding Engine failure behavior
- Charging profiles

## General APN Parameters

You configure these parameters to determine the servers that the broadband gateway contacts to authorize use, resolve domain names, and so forth. You also use these parameters to set timeout values for sessions or idle devices, and determine various other APN characteristics that do not fall into the other categories.

## Restriction Value

There are many types of APNs: some attach to service-rich public networks and others attach to more circumscribed private corporate networks. Restriction values can be placed on every APN on a broadband gateway to prevent unsupported inter-APN traffic from burdening the network and ending up useless at the destination.



## User Options

Anonymous users can use PDN services without logging in as specific users. A parameter, such as the APN name, can be used to distinguish and authorize the individual user, even if anonymous, on the network.

## Address Assignment

A key function of the broadband gateway is to assign IP addresses to mobile devices. These parameters establish the Dynamic Host Configuration Protocol (DHCP) family (IPv4 or IPv6) and pool to use for this APN.

## Anchor DPC or MPC Failure Behavior

All APN sessions run through a particular Dense Port Concentrator (DPC) or Modular Port Concentrator (MPC) on the broadband gateway, called the anchor PIC or Packet Forwarding Engine. These parameters control how the broadband gateway handles a session anchored on the DPC or MPC if it should fail.

## Charging Profiles

You configure charging profile parameters to determine how the broadband gateway charges home, roaming, and visiting users.

### Related Documentation

- [Configuring Address Assignment on a Broadband Gateway APN on page 122](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 135](#)
- [Configuring Charging, Local Policy, and Policy and Charging Enforcement Function Profiles on a Broadband Gateway APN on page 131](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 117](#)
- [Configuring Mobile Interfaces for APNs on page 133](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 134](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 121](#)
- [Configuring User Options on a Broadband Gateway APN on page 141](#)
- [Example: Configuring Broadband Gateway APNs on page 143](#)

---

## User-Session Routing Overview

The MobileNext Broadband Gateway supports user-session routing to dynamically redirect create session requests received on the broadband gateway to another mobile network gateway, when appropriate. You configure a service-selection profile on the broadband gateway to define the conditions that trigger a redirect action to reroute user sessions. The Broadband Gateway supports user-session routing for GTP v0, GTPv1, and GTPv2.

User-session routing is enabled on the broadband gateway when the configured service selection profile for the APN includes the **redirect-peer ip-address then** method. When a

create session request arriving on the broadband gateway triggers a redirect (the create session request indicates a match with one of the **from** conditions configured in service-selection profile), the broadband gateway off loads the create session request to another gateway on the mobile network that has the capability to service the create session request.

A broadband gateway might route a create session request to a more appropriate gateway to anchor create session requests in the following cases:

- A configured policy, session load, or system status (for example, maintenance mode) on the receiving broadband gateway adversely impacts the ability of the broadband gateway to service the create session request.
- A configuration on the broadband gateway prevents the gateway from meeting service, billing, or other requirements for the create session request.



**NOTE:** After a create session request is off loaded from the broadband gateway to another gateway (the broadband gateway receives a create session response), the broadband gateway has no further responsibility for the off-loaded subscriber session, and any subsequent data traffic or session modifications are handled by the new gateway.

---

The following sequence describes the call flow for user session routing:

1. The SGW sends a create session request (source IP SGW, destination IP PGW1, source port SGW1, destination port 2123)
2. PGW1 decides to redirect the request to PGW2
3. PGW1 sends the create session request to PGW2 (source IP PGW1, destination IP PGW2, source port PGW1, destination port 2123)
4. PGW2 sends a create session response to PGW1 (source IP PGW2, source port 2123, Destination IP PGW1, destination port PGW1)
5. PGW1 replies to SGW (source IP PGW1, source port 2123, destination IP SGW, destination port SGW)

In the preceding call flow sequence, PGW1 applies a service selection profile to a Create Session Request (at Step 2) to redirect the Create Session Request message to PGW2. PGW1 operates as a proxy for the SGW (at Step 3) by inserting its network address as an SGW network address within the Create Session Request. With PGW1 acting as a proxy, PGW2 can operate as if communicating with the SGW (at Step 4) according to conventional methods without having to support new functionality. Upon receiving a successful response from PGW2, PGW1 (at Step 5) sends a Create Session Response message to the SGW, directing the SGW to use PGW2 for future communications. As a result, any data and control traffic will travel directly between the SGW and PGW2 without any interaction from PGW1.

**Related Documentation**

- [Configuring APN Service Selection on a Broadband Gateway on page 135](#)
- [Configuring APNs on the MobileNext Broadband Gateway Overview on page 113](#)

## Configuring General APN Parameters on the Broadband Gateway

To configure an access point name (APN) on the MobileNext Broadband Gateway, you set general parameters for each APN. These APN parameters determine the servers the broadband gateway contacts to authorize use, resolve domain names, and so on. These parameters also set timeout values for sessions or idle devices, and determine various other APN characteristics.

This topic includes the following tasks:

- [Configuring the APN Name, Interface, and Type on page 117](#)
- [Configuring Servers for an APN on page 118](#)
- [Configuring APN Timers on page 119](#)
- [Configuring Miscellaneous APN Parameters on page 119](#)

### Configuring the APN Name, Interface, and Type

Before you begin configuring an APN on a broadband gateway, you should have done the following:

- Configured the chassis of the broadband gateway
- Configured the interfaces of the broadband gateway
- Configured the general Dynamic Host Configuration Protocol (DHCP) parameters for the broadband gateway

To configure an APN on the broadband gateway, you configure a name, mobile interface, and type for the APN. Each APN has one mobile interface that must be defined as a mobile interface on the broadband gateway chassis. To configure an APN:

1. Configure an APN name.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services]
user@host# set apn apn-1
```



**NOTE:** The APN name must be fewer than 80 characters and can contain letters, numbers, decimal points, and dashes only.

2. Configure a mobile interface for the APN.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1]
user@host# set mobile-interface mif-1/0/1.0
```



**NOTE:** The interface must be defined as a mobile interface (mif-) in the broadband gateway interface hierarchy.

3. Configure a type for the APN.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1]
```

```
user@host# set apn-type real
```



**NOTE:** APNs can be real, virtual, or virtual-pre-authenticate.

Select one of the following APN types:

- **real**—This APN type is used when the GPRS tunneling protocol (GTP) create message contains the APN name and is used to create the session.
- **virtual**—This APN type is used when the GTP create message contains an APN name, but the name must be mapped to a real APN. The mapping is done by configuring the service selection profile.
- **virtual-pre-authenticate**—This APN type, which is similar to a virtual APN, is used when the GTP create message contains an APN name that must be mapped to a real APN. However, the mapping in this case is done by RADIUS (you must configure RADIUS for this type of APN) during the authentication response (access accept message).



**NOTE:** When the APN type is virtual, anonymous users must still be authenticated. This action is included in the virtual-pre-authenticate APN type.

4. Configure a data type for the APN.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1]
user@host# set apn-data-type ipv4
```



**NOTE:** APNs can handle ipv4, ipv6, or ipv4v6 data. By default, APNs handle only IPv4 data.

## Configuring Servers for an APN

To configure a Domain Name System (DNS) server, NetBIOS name server (NBNS), or server to handle call session control for the APN:

1. Configure the IPv4 or IPv6 address of the primary and secondary DNS server.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1]
user@host# set dns-server primary 10.10.10.9 secondary 172.16.0.7
```

2. Configure the IPv4 or IPv6 address of the primary and secondary NBNS server.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1]
user@host# set nbns-server primary 192.168.27.48 secondary 10.10.9.222
```

3. Configure the IPv4 or IPv6 address of the call state control function (CSCF) server.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1]
user@host# set p-cscf-server 172.16.14.25
```

## Configuring APN Timers

To configure timers to control session or idle period timeouts:

1. Configure the session timeout.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1]
user@host# set session-timeout 0
```



**NOTE:** The range is 0 through 720 hours, with a default of 0 hours. A value of 0 hours means the session will never time out when active.

2. Configure the idle timeout.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1]
user@host# set idle-timeout 0
```



**NOTE:** The range is 0 through 300 minutes, with a default of 0 minutes. A value of 0 minutes means the session will never time out during idle periods.

3. Configure the idle timeout direction.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1]
user@host# set idle-timeout-direction both
```



**NOTE:** The direction can be both uplink or downlink, or idle detected in the uplink direction only. The default is to detect idle periods in both directions.

## Configuring Miscellaneous APN Parameters

To configure authorization profiles, inter-mobile traffic behavior, and various other parameters for the APN:

1. Configure the RADIUS authorization, authentication, and accounting (AAA) profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1]
user@host# set aaa-profile aaa-access-profile-1
```



**NOTE:** The RADIUS profile must be configured in the AAA hierarchy.

2. Configure inter-mobile device capabilities.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1]
user@host# set inter-mobile redirect 10.10.10.4
```



**NOTE:** You can deny mobile-to-mobile device traffic, or you can redirect it through another IP device address before delivery. The default is to allow mobile-to-mobile communication on the APN.

3. Configure the APN access selection method.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1]  
user@host# set selection-mode from-sgsn
```



**NOTE:**

The selection modes mean:

- **from-ms**—Admit subscribers with a mobile-station-provided APN without a verified subscription.
- **from-sgsn**—Admit subscribers with a network-provided APN without a verified subscription.
- **no-subscribed**—Reject subscribers with a mobile-station-provided or a network-provided APN, with a verified subscription.

4. Configure source address verification so the APN checks the validity of the mobile device source address.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1]  
user@host# set verify-source-address
```

5. Configure the maximum number of bearers (PDP contexts) allowed.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1]  
user@host# set maximum-bearers 1000000
```



**NOTE:** You can allow 100000 (one hundred thousand) to 12000000 (twelve million) bearers on the APN. There is no default.

6. Configure visitor blocking for this APN, which will prohibit visitors from accessing this APN (visitors are allowed by default). Visitors are defined as subscribers where the Serving GPRS Support Node (SGSN) or Serving Gateway (S-GW) belong to the same public land mobile network (PLMN), but the gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW) are in a different PLMN.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1]  
user@host# set block-visitors
```

7. Configure sessions to wait for accounting to engage for this APN (sessions do not wait by default).

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1]  
user@host# set wait-accounting
```

**Related Documentation**

- [Configuring Address Assignment on a Broadband Gateway APN on page 122](#)
- [Configuring APNs on the MobileNext Broadband Gateway Overview on page 113](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 135](#)
- [Configuring Charging, Local Policy, and Policy and Charging Enforcement Function Profiles on a Broadband Gateway APN on page 131](#)
- [Configuring Mobile Interfaces for APNs on page 133](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 134](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 121](#)
- [Configuring User Options on a Broadband Gateway APN on page 141](#)
- [Example: Configuring Broadband Gateway APNs on page 143](#)

## Configuring the Restriction Value on a Broadband Gateway APN

Access point names (APNs) serve different purposes in a mobile network. Some APNs attach mobile devices to public Packet Data Networks (PDNs) such as the Internet, while others attach mobile devices to private corporate networks. Different networks can have different capabilities and supported services. In many cases, the inter-mobile-device traffic for devices attached to different APNs must be restricted so that the network does not waste resources sending packets to a network that does not support them.

Before you begin configuring the restriction value on a MobileNext Broadband Gateway APN, you should have done the following:

- Configured the chassis of the broadband gateway
- Configured the interfaces of the broadband gateway
- Configured the general APN parameters for the specific APN

You configure the restriction value for an APN based on the applications allowed on this APN and on other APNs configured on the broadband gateway. When you configure the restriction value, users cannot, for example, send Multimedia Messaging Service (MMS) or Wireless Application Protocol (WAP) messages to a user on an APN that does not support MMS or WAP. [Table 15 on page 121](#) shows the maximum restriction value for an APN, the type of APN the restriction can apply to, application examples, and the restriction values allowed on other APNs. By default, there are no restrictions on traffic sent from one APN to another.

**Table 15: APN Restriction Values**

Maximum APN Restriction Value	Type of APN	Application Example	Allowed Restriction Values on Other APNs
0	NA	NA	Any
1	Public Type 1	WAP or MMS	1, 2, or 3

Table 15: APN Restriction Values (*continued*)

Maximum APN Restriction Value	Type of APN	Application Example	Allowed Restriction Values on Other APNs
2	Public Type 2	Internet or other PDN	1 or 2
3	Private Type 1	Corporate network MMS	1
4	Private Type 2	Corporate network without MMS	None

To configure the restriction value for an APN:

1. `[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1]  
user@host# set restriction-value 0`

#### Related Documentation

- [Configuring Address Assignment on a Broadband Gateway APN on page 122](#)
- [Configuring APNs on the MobileNext Broadband Gateway Overview on page 113](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 135](#)
- [Configuring Charging, Local Policy, and Policy and Charging Enforcement Function Profiles on a Broadband Gateway APN on page 131](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 117](#)
- [Configuring Mobile Interfaces for APNs on page 133](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 134](#)
- [Configuring User Options on a Broadband Gateway APN on page 141](#)
- [Example: Configuring Broadband Gateway APNs on page 143](#)

## Configuring Address Assignment on a Broadband Gateway APN

One of the key roles of the MobileNext Broadband Gateway configured as either a 3G Gateway GPRS Support Node (GGSN) or 4G Packet Data Network Gateway (P-GW) is to assign IP addresses to a mobile device. This topic configures the address assignment parameters for an access point name (APN).

Before you begin configuring address assignment on a broadband gateway APN, you should have done the following:

- Configured the chassis of the broadband gateway
- Configured the interfaces of the broadband gateway
- Configured the general APN parameters for the specific APN
- Configured the general Dynamic Host Configuration Protocol (DHCP) parameters for the broadband gateway



Devices accessing the broadband gateway APN can be assigned IP addresses in one of three ways: by the authentication, authorization, and accounting (AAA) server, by the DHCP server, or locally by the broadband gateway. In addition, you can configure the APN to accept static addresses that devices provide to the broadband gateway. When you configure an APN to assign addresses from the AAA server or locally on the broadband gateway, or to accept static addresses provided by the device (user equipment), you must configure the IP addresses in a mobile pool on the broadband gateway, otherwise the subscriber sessions are rejected.



**NOTE:** Configuring address assignment on an APN is optional. If you do not configure an address assignment method for an APN, then the broadband gateway assigns IP addresses for that APN using the configured default mobile pool.

To configure address assignment on a broadband gateway APN:

1. Specify that you want to configure address assignment on an APN named `apn-1` in a broadband gateway named `MBG1`.

```
user@host# edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1  
address-assignment
```

2. (Optional) Specify that the AAA server assigns IP addresses to subscribers.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1  
address-assignment]  
user@host# set aaa
```

**NOTE:**

- If you include the `aaa` statement, you cannot include the `dhcp-proxy-client` or `local` statements. The configuration in the AAA profile specified for the APN determines the AAA server that will assign addresses to subscribers.
- The IP address assigned by the AAA server must be previously configured on the gateway either in a mobile pool or a mobile pool group at the `[edit access address-assignment]` or `[edit routing-instances instance-name access address-assignment]` hierarchy levels. In addition, the mobile pool must be configured as external assigned by including the `external-assigned` statement at the `[edit access address-assignment mobile-pools]` or the `[edit routing-instances instance-name access address-assignment mobile-pools]` hierarchy levels.
- For IPv4 addresses, the AAA server must be configured to send the IPv4 address in the Framed-IP-Address attribute-value pair (AVP) in the Access Accept Response message to the broadband gateway; for example, the Framed-IP-Address AVP can be set to "192.168.0.10".
- For IPv6 addresses, the AAA server must be configured to send the IPv6 address in the Framed-IPv6-Prefix AVP in the Access Accept Response message to the broadband gateway; for example, the Framed-IPv6-Prefix AVP can be set to "2000:DB8::".

3. (Optional) Configure the APN so that the IP subnet returned by the DHCP server is used by the broadband gateway to assign IP addresses to subscribers.
- a. Specify that the broadband gateway uses the information configured in the DHCP proxy client profile to obtain the IP subnet returned by the DHCP server.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1  
address-assignment]  
user@host# set dhcp-proxy-client
```



**NOTE:** If you include the `dhcp-proxy-client` statement, you cannot include the `aaa` or `local` statements. In addition, you must configure a DHCPv4 proxy client profile, a DHCPv6 proxy client profile, or both profiles, depending on the type of addresses that the APN can allocate (configured in the `apn-data-type` statement).

- b. (Optional) Specify that the IP address returned by the AAA server overrides the address from the subnet returned from the DHCP server. In this case, if the AAA server provides an IP address for the user equipment, then the gateway does not assign an address from the subnet, which is returned from the DHCP server for the APN.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1  
address-assignment]  
user@host# set dhcp-proxy-client aaa-override
```

**NOTE:**

- If the AAA server assigns the IP address, then that IP address must be previously configured on the gateway either in a mobile pool or a mobile pool group at the [edit access address-assignment] or [edit routing-instances instance-name access address-assignment] hierarchy levels. In addition, the mobile pool must be configured as external assigned by including the external-assigned statement at the [edit access address-assignment mobile-pools] or the [edit routing-instances instance-name access address-assignment mobile-pools] hierarchy levels.
- In addition, the AAA server must be configured to send the IP address, in the Framed-IP-Address AVP (for IPv4 addresses) or the Framed-IPv6-Prefix AVP (for IPv6 addresses), as part of the Access Accept Response message to the broadband gateway. For example, the Framed-IP-Address AVP can be set to “192.168.0.10” for IPv4, and the Framed-IPv6-Prefix AVP can be set to “2000:DB8::” for IPv6.

- c. Specify the name of the DHCPv4 proxy client profile for the APN.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
address-assignment]
user@host# set dhcpv4-proxy-client-profile profile-name profile-name
```



**NOTE:** If the `apn-data-type` is set to `ipv4` or `ipv4v6` and if you have included the `dhcp-proxy-client` statement, you must specify a DHCPv4 proxy client profile name for the APN.

The DHCPv4 proxy client profile must be previously configured at the [edit routing-instances name system dhcp-proxy-client] or the [edit system dhcp-proxy-client] hierarchy levels.

- d. (Optional) Configure the logical system for the DHCPv4 proxy client profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
address-assignment]
user@host# set dhcpv4-proxy-client-profile logical-system logical-system-name
```



**NOTE:** This is the logical system where the DHCPv4 proxy client profile is defined. If this is not specified, the default logical system is used.

- e. (Optional) Specify the name of the address pool for the DHCPv4 proxy client profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
address-assignment]
user@host# set dhcpv4-proxy-client-profile pool-name pool-name
```



**NOTE:** The specified address pool name is sent to the DHCP server.

- f. (Optional) Configure the routing instance for the DHCPv4 proxy client profile to use for this APN.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
 address-assignment]
user@host# set dhcpv4-proxy-client-profile routing-instance routing-instance-name
```

- g. Specify the name of the DHCPv6 proxy client profile for the APN.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
 address-assignment]
user@host# set dhcpv6-proxy-client-profile profile-name profile-name
```



**NOTE:** If the `apn-data-type` is set to `ipv6` or `ipv4v6` and if you have included the `dhcp-proxy-client` statement, you must specify a DHCPv6 proxy client profile name for the APN.

The DHCPv6 proxy client profile must be previously configured at the `[edit routing-instances name system dhcp-proxy-client]` or the `[edit system dhcp-proxy-client]` hierarchy levels.

- h. (Optional) Configure the logical system for the DHCPv6 proxy client profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
 address-assignment]
user@host# set dhcpv6-proxy-client-profile logical-system logical-system-name
```



**NOTE:** This is the logical system where the DHCPv6 proxy client profile is defined. If this is not specified, the default logical system is used.

- i. (Optional) Configure the address pool name for the DHCPv6 proxy client profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
 address-assignment]
user@host# set dhcpv6-proxy-client-profile pool-name pool-name
```



**NOTE:** The specified address pool name is sent to the DHCP server.

- j. (Optional) Configure the routing instance for the DHCPv6 proxy client profile to use for this APN.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
 address-assignment]
user@host# set dhcpv6-proxy-client-profile routing-instance routing-instance-name
```

4. (Optional) Configure the APN so that the broadband gateway assigns IP addresses to subscribers.

- a. Specify that the broadband gateway assigns IP addresses to subscribers.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
 address-assignment]
user@host# set local
```



**NOTE:** If you include the `local` statement, you cannot include the `aaa` or `dhcp-proxy-client` statements.

- b. (Optional) Specify that the IP address returned by the AAA server overrides the address assigned by the broadband gateway. In this case, if the AAA server provides an IP address for the user equipment, then the gateway does not assign an IP address.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
 address-assignment]
user@host# set local aaa-override
```



**NOTE:**

- If the AAA server assigns the IP address, then that IP address must be previously configured on the gateway either in a mobile pool or a mobile pool group at the `[edit access address-assignment]` or `[edit routing-instances instance-name access address-assignment]` hierarchy levels. In addition, the mobile pool must be configured as external assigned by including the `external-assigned` statement at the `[edit access address-assignment mobile-pools]` or the `[edit routing-instances instance-name access address-assignment mobile-pools]` hierarchy levels.
- In addition, the AAA server must be configured to send the IP address, in the Framed-IP-Address AVP (for IPv4 addresses) or the Framed-IPv6-Prefix AVP (for IPv6 addresses), as part of the Access Accept Response message to the broadband gateway. For example, the Framed-IP-Address AVP can be set to “192.168.0.10” for IPv4, and the Framed-IPv6-Prefix AVP can be set to “2000:DB8::” for IPv6.

5. (Optional) Specify the IPv4 mobile pool or mobile pool group from which IPv4 addresses are assigned to subscribers. The mobile pool or mobile pool group must be previously configured at the `[edit access address-assignment]` or `[edit routing-instances instance-name access address-assignment]` hierarchy level.



**NOTE:** You can specify an IPv4 mobile pool or mobile pool group if the `apn-data-type` is set to `ipv4` or `ipv4v6`, and if one of the following conditions is valid:

- The `aaa` statement is included at the [edit unified-edge gateways `ggsn-pgw gateway-name apn-services apns apn-name address-assignment`] hierarchy level.
- The `aaa-override` statement is included at the [edit unified-edge gateways `ggsn-pgw gateway-name apn-services apns apn-name address-assignment dhcp-proxy-client`] hierarchy level.
- The `local` statement is included at the [edit unified-edge gateways `ggsn-pgw gateway-name apn-services apns apn-name address-assignment`] hierarchy level.

- a. Specify the name of the IPv4 mobile pool, for the APN, from which addresses are assigned to subscribers.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
 address-assignment]
user@host# set inet-pool pool pool-name
```

- b. (Optional) Specify the name of the IPv4 mobile pool group, for the APN, from which addresses are assigned to subscribers.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
 address-assignment]
user@host# set inet-pool group group-name
```



**NOTE:** You can specify a mobile pool or a mobile pool group for an APN, but not both.

- c. (Optional) Specify the names of the IPv4 mobile pools, for the APN, that will be excluded from the specified mobile pool group. IP addresses will not be assigned from the specified pools.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
 address-assignment]
user@host# set inet-pool exclude-pools pool-name
```

You can specify more than one mobile pool to exclude using a single `set` statement and enclosing the names of the pool in square brackets (`[]`). For example, to exclude two pools, `pool-A` and `pool-B`, from the mobile pool group `mbg-group-1`:

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
 address-assignment]
user@host# set inet-pool exclude-pools [pool-A pool-B]
```

6. (Optional) Specify the IPv6 mobile pool or mobile pool group from which IPv6 addresses are assigned to subscribers. The mobile pool or mobile pool group must be previously configured at the [edit access address-assignment] or [edit routing-instances `instance-name access address-assignment`] hierarchy level.



**NOTE:** You can specify an IPv6 mobile pool or mobile pool group if the `apn-data-type` is set to `ipv6` or `ipv4v6` and if one of the following conditions is valid:

- The `aaa` statement is included at the [edit unified-edge gateways `ggsn-pgw gateway-name apn-services apns apn-name address-assignment`] hierarchy level.
- The `aaa-override` statement is included at the [edit unified-edge gateways `ggsn-pgw gateway-name apn-services apns apn-name address-assignment dhcp-proxy-client`] hierarchy level.
- The `local` statement is included at the [edit unified-edge gateways `ggsn-pgw gateway-name apn-services apns apn-name address-assignment`] hierarchy level.

- a. Specify the name of the IPv6 mobile pool, for the APN, from which addresses are assigned to subscribers.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
address-assignment]
user@host# set inet6-pool pool pool-name
```

- b. (Optional) Specify the name of the IPv6 mobile pool group, for the APN, from which addresses are assigned to subscribers.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
address-assignment]
user@host# set inet6-pool group group-name
```



**NOTE:** You can specify a mobile pool or a mobile pool group for an APN but not both.

- c. (Optional) Specify the names of the IPv6 mobile pools, for the APN, that will be excluded from the specified mobile pool group. IP addresses will not be assigned from the specified pools.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
address-assignment]
user@host# set inet6-pool exclude-v6pools pool-name
```

You can specify more than one mobile pool to exclude using a single `set` statement and enclosing the names of the pool in square brackets (`[]`). For example, to exclude two pools, `pool-A` and `pool-B`, from the mobile pool group `mbg-group-1`:

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
address-assignment]
user@host# set inet6-pool exclude-v6pools [pool-A pool-B]
```

7. (Optional) Specify that the static IP address provided by the user equipment (UE) is allowed by the broadband gateway. The gateway obtains the IP address of the user equipment from the Create PDP Context or Create Session Request message.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1  
address-assignment]  
user@host# set allow-static-ip-address
```



**NOTE:** If you do not include the `allow-static-ip-address` statement, then the broadband gateway does not allow static IP address provided by the user equipment.

- a. (Optional) Specify that the static IP address provided by the user equipment is not verified with the AAA server during the authentication phase.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1  
address-assignment]  
user@host# set allow-static-ip-address no-aaa-verify
```



**NOTE:** If you do not include the `no-aaa-verify` statement, then the static IP address provided by the user equipment is verified by the AAA server during the authentication phase. This occurs if an AAA profile is configured for the APN and if authentication is enabled in the AAA profile.

#### Related Documentation

- [address-assignment \(APN\)](#)
- [address-assignment \(MobileNext Broadband Gateway\)](#)
- [Configuring APNs on the MobileNext Broadband Gateway Overview on page 113](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 135](#)
- [Configuring Charging, Local Policy, and Policy and Charging Enforcement Function Profiles on a Broadband Gateway APN on page 131](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 117](#)
- [Configuring Mobile Interfaces for APNs on page 133](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 134](#)
- [Configuring Mobile Pools and Mobile Pool Groups on the Broadband Gateway on page 230](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 121](#)
- [Configuring User Options on a Broadband Gateway APN on page 141](#)
- [Example: Configuring Broadband Gateway APNs on page 143](#)



## Configuring Charging, Local Policy, and Policy and Charging Enforcement Function Profiles on a Broadband Gateway APN

The Mobile Next Broadband Gateway applies different charging profiles to different types of users.

Before you begin configuring charging profiles on a broadband gateway access point network (APN), you should have done the following:

- Configured the chassis of the broadband gateway
- Configured the interfaces of the broadband gateway
- Configured the general APN parameters for the specific APN
- Configured the charging profiles, quality-of-service (QoS) local policy profile, and policy and charging enforcement function (PCEF) profile for the broadband gateway

To assign charging profiles to various types of users accessing an APN on the broadband gateway, you associate a user type with a charging profile name. The charging profile details for the APN users must be configured first. The default charging profile is used when a more specific profile does not apply. To assign local policy profiles for QoS purposes to an APN, you reference the name of the local policies group and its member profiles in the APN.

Based on a comparison of public land mobile networks (PLMNs), the mobile user falls into one of three categories:

- Home user—The subscriber, the gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW), and Serving GPRS Support Node (SGSN) or Serving Gateway (S-GW) are all in the same PLMN.
- Roaming user—The subscriber and GGSN or P-GW belong to the same PLMN, but the SGSN or S-GW are in a different PLMN.
- Visiting user—The subscriber and SGSN or S-GW belong to the same PLMN, but the GGSN or P-GW are in a different PLMN.

To configure charging profiles on a broadband gateway APN:

1. Configure the default charging profile that is used by **apn-1** when no other profile applies.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1 charging]
user@host# set default-charging-profile default-charging-profile-apn-1
```

2. Configure the home user's charging profile for **apn-1**.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1 charging]
user@host# set home-charging-profile home-charging-profile-apn-1
```

3. Configure the roaming user's charging profile for **apn-1**.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1 charging]
user@host# set roamer-charging-profile roamer-charging-profile-apn-1
```

4. Configure the visiting user's charging profile for **apn-1**.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1 charging]
user@host# set visitor-charging-profile visitor-charging-profile-apn-1
```

5. Configure the broadband gateway to select the charging profile sent by the SGSN or S-GW first, sent by the RADIUS server next, or use the charging profiles statically configured locally for **apn-1**. These three options work in order you enter them.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1 charging]
user@host# set profile-selection-order serving
user@host# set profile-selection-order radius
user@host# set profile-selection-order static
```



**NOTE:** You do not have to use all three options.

6. Configure a local policy profile to define the quality of service (QoS) treatment for the default bearer associated with **apn-1**:

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1 charging]
user@host# set local-policy-profile local-policy-1
```



**NOTE:** A local policy configured for an APN specifies the QoS treatment for default bearers when no PCEF profile is configured on the APN. If both a local policy profile and a PCEF profile for static policies are configured on the APN, the local policy specifies the QoS treatment for the default bearer and the PCEF profile specifies the QoS and charging treatment for the dedicated bearers. If both a local policy and a PCEF profile for dynamic policies are configured on the APN, the policy and charging rules function (PCRF) interacts with the PCEF to determine the QoS and charging treatment for both the default and dedicated bearers, and the local policy profile is ignored.

7. Configure a PCEF profile to define the QoS, charging, and gating control for IP flows (as specified in the Policy and Charging Control (PCC) rules) for **apn-1**:

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1 ]
user@host# set pcef-profile pcef-profile1
```

#### Related Documentation

- [Configuring Address Assignment on a Broadband Gateway APN on page 122](#)
- [Configuring APNs on the MobileNext Broadband Gateway Overview on page 113](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 135](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 117](#)
- [Configuring Mobile Interfaces for APNs on page 133](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 134](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 121](#)
- [Configuring User Options on a Broadband Gateway APN on page 141](#)

- [Example: Configuring Broadband Gateway APNs on page 143](#)

## Configuring Mobile Interfaces for APNs

You configure the MobileNext Broadband Gateway with mobile interfaces (**mif-**) for access point name (APN) traffic. The mobile interfaces are distinct from other type of interfaces and are used to associate an APN with a physical interface in a virtual routing and forwarding table (VRF). You need to configure one mobile interface unit for every APN. Every APN is associated with a single logical interface (unit) on a physical port represented by a mobile interface unit.

Before you begin, you should have done the following:

- Installed the broadband gateway
- Installed the boards of the broadband gateway
- Decided how many initial or additional APNs are required (you can add APNs after initial configuration)

To configure a mobile interface for mobility, you configure one or more logical interfaces (units) for the interface:

1. Configure the logical interface.

```
[edit interfaces]
user@host# set mif unit 0 family inet
```

2. Optionally, configure the maximum transmission unit (MTU) size for the mobile interface.

```
[edit interfaces]
user@host# set mif mtu 1200
```



**NOTE:** MTU sizes are not mobility specific. However, MTU size is important because the GPRS tunneling protocol (GTP) header can cause a data unit to exceed the maximum frame size when the tunnel headers are added. This causes an error.

3. Optionally, configure the access control list (ACL) filters to apply to uplink and downlink traffic. By default, the APN accepts all mobile traffic. You can selectively accept or reject mobile traffic based on filter actions.

```
[edit interfaces]
user@host# set mif unit 0 filter input input-mif-unit0-filter
user@host# set mif unit 0 filter output output-mif-unit0-filter
```



**NOTE:** Filter configuration is not covered as part of mobility topics. The filtering is not mobility specific.

4. Optionally, configure the service filters to apply to uplink and downlink traffic at the APN level. Typically, these filters would provide services such as Network Address translation (NAT) to mobile traffic. By default, no such services are applied to mobile traffic:

[edit interfaces]

```
user@host# set mif unit 0 service input service-filter input-service-unit0 service-set  
nat-service-unit0
```

```
user@host# set mif unit 0 service output service-filter input-service-unit0 service-set  
nat-service-unit0
```



**NOTE:** Service filter configuration is not covered as part of mobility topics. Service filtering is not mobility specific.

---

#### Related Documentation

- [Configuring Address Assignment on a Broadband Gateway APN on page 122](#)
- [Configuring APNs on the MobileNext Broadband Gateway Overview on page 113](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 135](#)
- [Configuring Charging, Local Policy, and Policy and Charging Enforcement Function Profiles on a Broadband Gateway APN on page 131](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 117](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 134](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 121](#)
- [Configuring User Options on a Broadband Gateway APN on page 141](#)
- [Example: Configuring Broadband Gateway APNs on page 143](#)

---

## Configuring Mobile Interface to APN Associations in VRFs

The MobileNext Broadband Gateway associates mobile interfaces (**mif-**) with access point names (APNs). Every APN is associated with a single logical interface (unit) on a physical port represented by a mobile interface unit. The mapping of the mobile interface to physical interface is usually done in a virtual routing and forwarding (VRF) table. Using a VRF for each APN allows isolation of routing information and protocols by customer and simplifies gateway operation.

Before you begin, you should have done the following:

- Installed the broadband gateway
- Installed the boards of the broadband gateway
- Configured the physical interfaces on the broadband gateway chassis (this process is not mobility-specific)
- Configured the mobility interfaces on the broadband gateway chassis

To configure a mobility-interface-to-APN mapping in a VRF, specify the VRF and place both the mobile logical interface (unit) and the physical interface unit (the Gi or SGi interface for the APN) in the same VRF. This procedure places **mif.1** and **ge-0/0/0.5** in a VRF called **User1-VRF** and places **mif.2** and **ge-0/0/0.0** in a VRF called **User2-VRF**.

1. Configure the mobility logical interface for **User1-VRF**:

```
[edit routing-instances]
user@host# set User1-VRF interface mif.1
user@host# set User1-VRF interface ge-0/0/0.5
```

2. Configure the mobility logical interface for **User2-VRF**:

```
[edit routing-instances]
user@host# set User2-VRF interface mif.2
user@host# set User2-VRF interface ge-0/0/0.0
```



**NOTE:** Normally, you would configure more statements for a VRF, but those additional statements are not mobility specific and not covered here.

#### Related Documentation

- [Configuring Address Assignment on a Broadband Gateway APN on page 122](#)
- [Configuring APNs on the MobileNext Broadband Gateway Overview on page 113](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 135](#)
- [Configuring Charging, Local Policy, and Policy and Charging Enforcement Function Profiles on a Broadband Gateway APN on page 131](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 117](#)
- [Configuring Mobile Interfaces for APNs on page 133](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 121](#)
- [Configuring User Options on a Broadband Gateway APN on page 141](#)
- [Example: Configuring Broadband Gateway APNs on page 143](#)

## Configuring APN Service Selection on a Broadband Gateway

The MobileNext Broadband Gateway can select an access point name (APN) in various ways. You configure a service selection profile as an “if-then” construction similar to other Junos OS policies using **from** and **then** statements.

Before you begin configuring service selection on a broadband gateway APN, you should have done the following:

- Configured the chassis of the broadband gateway
- Configured the interfaces of the broadband gateway
- Configured the APN parameters for the specific APN

To configure a service selection profile, you can choose one or more of the following **from** conditions:

- **anonymous-user**—Match anonymous users.
- **charging-characteristics value**—Match the charging characteristics value from 0 through 65,535.
- **domain-name domain-name**—Match the domain name.
- **imei imei-prefix**—Match the International Mobile Equipment Identity (IMEI) prefix configured.
- **imsi imsi-prefix**—Match the International Mobile Subscriber Identity (IMSI) prefix configured.
- **maximum-bearers value**—Match the number of bearers in the gateway from 1 through 10,000,000 (10 million).
- **msisdn msisdn-number-prefix**—Match the Mobile Station Integrated Services Digital Network (MSISDN) prefix configured.
- **pdn-type (ipv4 | ipv6 | ipv4v6)**—Match the IP version configured.
- **peer ip-address**—Match the IP address of the peer creating the session.
- **peer-routing-instance routing-instance-name**—Match the routing instance to which the peer creating the session is connected.
- **plmn**—Match the public land mobile network (PLMN). You can specify the following attributes for the PLMN:
  - **except**—Match all the PLMNs except the PLMNs specified in this match condition.
  - **mcc mcc mnc mnc**—Match the PLMN specified, if the **except** statement is not configured.
- **rat-type (eutran | geran | hspa | utran | wlan)**—Match the type of Radio Access Technology (RAT).
- **roaming-status (home | roamer | visitor)**—Match the subscriber's roaming status.



**NOTE:** Multiple terms can be configured in a service selection profile, and each term is applied in the order in which it is configured. Furthermore, multiple match conditions can be specified within a term and all of the conditions have to match. Once a matching term is found, the action is applied and no further terms are matched. If no term matches for a subscriber, then the services associated with the APN in the Create Session Request message are applied.

If the **charging-profile**, **pcef-profile**, or both actions are configured for a term, then the configured actions override the corresponding default services associated with the APN in the Create Session Requests that match the term.

---

To configure a service selection profile, you can choose one of the following **then** actions:

- **accept**—Accept the connection that matches the term.
- **apn-name *apn-name***—Select this real APN name.
- **charging-profile *charging-profile-name***—Select this charging profile.
- **pcef-profile *pcef-profile-name***—Select this policy and charging enforcement function (PCEF) profile.
- **redirect-peer *ip-address***—Select this redirected peer address to access the APN.
- **reject**—Reject the connection that matches the term.

To configure service selection profile **from** statements on a broadband gateway:

1. Configure the **anonymous-user from** method in a term called *select-apn* in a service selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles apn-1-selection
term select-apn]
user@host# set from anonymous-user
```



**NOTE:** Terms can be up to 63 characters long.

2. Configure the **charging-characteristics from** method in a term called *select-apn* in a service selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles apn-1-selection
term select-apn]
user@host# set from charging-characteristics 12345
```

3. Configure the **domain-name from** method in a term called *select-apn* in a service selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles apn-1-selection
term select-apn]
user@host# set from domain-name www.juniper.net
```

4. Configure the **imei from** method in a term called *select-apn* in a service selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles apn-1-selection
term select-apn]
user@host# set from imei imei-number-prefix
```



**NOTE:** The IMEI prefix matches the specified digits. For example, from imei 12345 matches the first five digits as given, then any other digits.

5. Configure the **imsi from** method in a term called *select-apn* in a service selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles apn-1-selection
term select-apn]
```

```
user@host# set from imsi imsi-number-prefix
```



**NOTE:** The IMSI prefix matches the specified digits. For example, from imsi 1222 matches the first four digits as given, then any other digits.

6. Configure the **maximum-bearers from** method in a term called *select-apn* in a service selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles apn-1-selection
term select-apn]
```

```
user@host# set from maximum-bearers 123456
```

7. Configure the **msisdn from** method in a term called *select-apn* in a service selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles apn-1-selection
term select-apn]
```

```
user@host# set from msisdn msisdn-number-prefix
```



**NOTE:** The MSISDN prefix matches the specified digits. For example, from msisdn 1212555 matches the first seven digits as given, then any other digits.

8. Configure the **pdn-type from** method in a term called *select-apn* in a service selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles apn-1-selection
term select-apn]
```

```
user@host# set from pdn-type ipv4
```



**NOTE:** The PDN type can be IPv4, IPv6, or both IPv4 and IPv6.

9. Configure the **peer from** method in a term called *select-apn* in a service selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles apn-1-selection
term select-apn]
```

```
user@host# set from peer 192.168.1.20
```

10. Configure the **peer-routing-instance from** method in a term called *select-apn* in a service selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles apn-1-selection
term select-apn]
```

```
user@host# set from peer-routing-instance mobility-instance
```

11. Configure the **plmn from** method in a term called *select-apn* in a service selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles apn-1-selection
term select-apn]
```

```
user@host# set from plmn except
```

```
user@host# set from plmn mcc mcc mnc mnc
```



**NOTE:**

- If you configure the **except** statement, then all PLMNs except the ones specified here are matched.
- You can specify more than one PLMN by including the **set mcc *mcc* mnc *mnc*** command multiple times.

12. Configure the **rat-type from** method in a term called *select-apn* in a service selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles apn-1-selection
term select-apn]
user@host# set from rat-type eutran
```



**NOTE:** The RAT type can be E-UTRAN, GERAN, HSPA, UTRAN, or WLAN.

13. Configure the **roaming-status from** method in a term called *select-apn* in a service selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles apn-1-selection
term select-apn]
user@host# set from roaming-status home
```



**NOTE:** The subscriber's roaming status can be home, roamer, or visitor.

To configure service selection profile **then** statements on a broadband gateway:

1. Configure the **accept then** method in a term called *select-apn* in a service selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles apn-1-selection
term select-apn]
user@host# set then accept
```



**NOTE:** If you configure the **accept** statement, then the following is applicable:

- No other actions can be configured for the term.
- Matching of subsequent terms is stopped and the services associated with the APN in the Create Session Request message are applied to the connection that matches the term.

2. Configure the **apn-name then** method in a term called *select-apn* in a service selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles apn-1-selection
term select-apn]
user@host# set then apn-name MBG1-apn
```

3. Configure the **charging-profile then** method in a term called *select-apn* in a service selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles apn-1-selection
term select-apn]
user@host# set then charging-profile charging-profile-name
```



**NOTE:** The charging profile must be previously configured on the broadband gateway at the [edit unified-edge gateways ggsn-pgw *gateway-name* charging] hierarchy level.

4. Configure the **pcef-profile then** method in a term called *select-apn* in a service selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles apn-1-selection
term select-apn]
user@host# set then pcef-profile pcef-profile-name
```



**NOTE:** The PCEF profile must be configured on the broadband gateway at the [edit unified-edge pcef] hierarchy level.

5. Alternatively, configure the **redirect-peer then** method in a term called *select-apn* in a service selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles apn-1-selection
term select-apn]
user@host# set then redirect-peer 192.168.20.1
```



**NOTE:** If you configure the **redirect-peer** statement, then no other actions can be configured for the term.

6. Configure the **reject then** method in a term called *select-apn* in a service selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles apn-1-selection
term select-apn]
user@host# set then reject
```



**NOTE:** If you configure the **reject** statement, then the following is applicable:

- No other actions can be configured for the term.
- Matching of subsequent terms is stopped and all connections that matched the term are rejected.

#### Related Documentation

- [Configuring Address Assignment on a Broadband Gateway APN on page 122](#)
- [Configuring APNs on the MobileNext Broadband Gateway Overview on page 113](#)

- [Configuring Charging, Local Policy, and Policy and Charging Enforcement Function Profiles on a Broadband Gateway APN on page 131](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 117](#)
- [Configuring Mobile Interfaces for APNs on page 133](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 134](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 121](#)
- [Configuring User Options on a Broadband Gateway APN on page 141](#)
- [Example: Configuring Broadband Gateway APNs on page 143](#)

---

## Configuring User Options on a Broadband Gateway APN

---

Before you begin configuring the user options on a MobileNext Broadband Gateway access point name (APN), you should have done the following:

- Configured the chassis of the broadband gateway
- Configured the interfaces of the broadband gateway
- Configured the general APN parameters for the specific APN

Users on the broadband gateway APN are authenticated using the authentication, authorization, and accounting (AAA) profile configured for the APN, if authentication is enabled in the AAA profile. The gateway determines the subscriber's username and password using the Protocol Configuration Options (PCO) Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) information received in the Create packet data protocol (PDP) Context Request or a Create Session Request message. For anonymous users, however, the gateway does not receive the PCO PAP or CHAP information in the Create PDP Context Request or Create Session Request message. By default, anonymous users are rejected by the gateway.

To authenticate anonymous users on a broadband gateway APN, you must configure a default username and password (using the `user-options` statement) for authentication. When the gateway receives a Create PDP Context Request or a Create Session Request message without the PCO PAP or CHAP information, the user options configured for the APN are used for user authentication with the AAA server. Instead of specifying a default username, you can specify that the device's International Mobile Station Identity (IMSI), Mobile Subscriber Integrated Services Digital Network (MSISDN) number, or APN name is used as the username to authenticate users. In addition, you can also specify (using the `override-pco` statement) that all users are authenticated on the APN using the configured default username and password.

To configure user options parameters on a broadband gateway APN:

1. Configure the default username to be used to authenticate anonymous users or all users (if the `override-pco` statement is configured) on `apn-1`.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1 user-options]  
user@host# set user-name user-name
```



**NOTE:** Alternatively, you can configure the gateway to use the MSISDN (set `use-msdn`), the APN name (set `use-apnname`), or the IMSI (set `use-imsi`) as the username for authentication. There is no default username.

2. Configure the password to be used to authenticate for anonymous users or all users (if the `override-pco` statement is configured) on `apn-1`.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1 user-options]
user@host# set password password
```

For example, to configure the password `2*201s550`:

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1 user-options]
user@host# set password 2*201s550
```



**NOTE:** The password can be up to 32 characters long, and it is stored encrypted.

3. Specify that the username and password configured for the APN override the username and password obtained from the PCO PAP or CHAP.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1 user-options]
user@host# set pco-override
```



**NOTE:** If you configure this statement you must configure a username and password.

#### Related Documentation

- [Configuring Address Assignment on a Broadband Gateway APN on page 122](#)
- [Configuring APNs on the MobileNext Broadband Gateway Overview on page 113](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 135](#)
- [Configuring Charging, Local Policy, and Policy and Charging Enforcement Function Profiles on a Broadband Gateway APN on page 131](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 117](#)
- [Configuring Mobile Interfaces for APNs on page 133](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 134](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 121](#)
- [Example: Configuring Broadband Gateway APNs on page 143](#)
- *user-options (APN)*

## Example: Configuring Broadband Gateway APNs

This example shows how to configure an access point name (APN) on the MobileNext Broadband Gateway. The APN interfaces, including the mobile interface (**mif-**), are placed into a virtual routing and forwarding (VRF) routing instance.

- [Requirements on page 143](#)
- [Overview on page 143](#)
- [Configuration on page 144](#)
- [Verification on page 146](#)

### Requirements

This example uses the following hardware and software components:

- An MX chassis equipped with session Dense Port Concentrators (DPCs) and three interface PFEs (housed in Modular Port Concentrators [MPCs]).
- The Junos OS Mobility package software

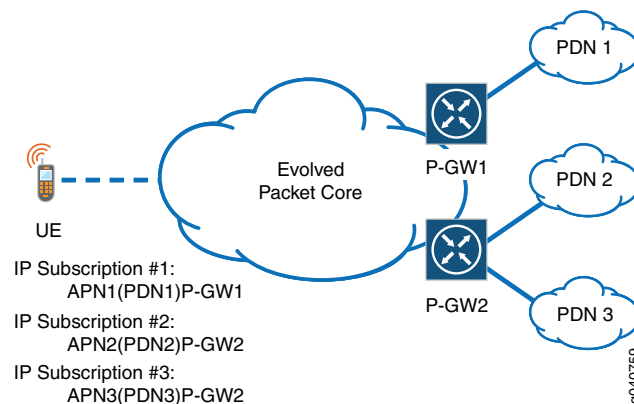
Before you begin:

- Install the chassis hardware.
- Configure the chassis, as well as interfaces, anchor Session PICs and anchor PFEs, and (optionally) redundancy.

### Overview

[Figure 36 on page 143](#) shows the role of APNs in a 4G network (APNs apply to other mobile network generations as well). APNs contain the parameters used to characterize a user session with a packet network. The broadband gateway uses the APN to identify an attached IP network.

**Figure 36: APNs Connect Mobile Devices to IP Networks Through a P-GW**



In this example, the broadband gateway has only one APN configured. Not all parameters are configured in this example, and many of them document default values (this is not an unusual practice: the default values are now clearly visible to all). All mobile devices attach to this APN. The mobile interface is configured and then the interfaces for the APN are placed in a separate VRF.

In detail, the broadband gateway is named **MBG1** and the APN is called **apn-1**. The MIF interface is configured as **mif.0** and is a real APN. The APN includes Domain Name System (DNS) and proxy call session control function (P-CSCF) servers. All timers use the default values, and includes an authentication, authorization, and accounting (AAA) profile called **aaa-access-profile-1** (this profile is configured under the unified-edge AAA mobility hierarchy level). All other general APN parameters either use the default values or are not configured.

This APN configuration places no restrictions on inter-mobile traffic sent within the APN (this is the default). The APN supports only IPv4 and the address assignment method uses the default timer value (0) so that addresses can be re-used immediately. The address pool is called **pool-1** (you can configure a pool or group, but not both for an APN). No pools are excluded.

The APN references only the default charging profile. The APN configures one MIF interface (taking all default values) called **mif.0** and associates the mobile interface and the local IP interface (Gi or SGI: in this case **ge-0/0/0.5**) in a VRF called **User1-VRF**. (No other VRF parameters are shown.) The APN service selection method (called **apn-1-selection**) takes the most inclusive **from** (a blank clause) in term **select-apn** and assigns all traffic to **apn-1**.

## Configuration

### CLI Quick Configuration

The APN referenced above is configured by:

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services]
user@host# set apn apn-1

[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1]
user@host# set mobile-interface mif.0
user@host# set apn-type real
user@host# set apn-data-type ipv4
user@host# set dns-server primary-v4 10.10.10.9 secondary-v4 172.16.0.7
user@host# set p-cscf 172.16.14.25
user@host# set session-timeout 0
user@host# set idle-timeout 0
user@host# set idle-timeout-direction both
user@host# set aaa-profile aaa-access-profile-1
user@host# set restriction-value 0

[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
  address-assignment-method]
user@host# set aaa
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1 address-assignment
  inet-pool]
user@host# set pool pool-1
```

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1 charging]
user@host# set default-charging-profile default-charging-profile-apn-1
```

```
[edit interfaces]
user@host# set mif unit 0 family inet
```

```
[edit routing-instances]
user@host# set User1-VRF interface mif.0
user@host# set User1-VRF interface ge-0/0/0.5
```

**Results** From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, these **show** command outputs include only the configuration that is relevant to this example.

```
user@MBG1# show unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
mobile-interface mif.0;
apn-type real;
apn-data-type ipv4;
dns-server primary 10.10.10.p secondary 172.16.0.7;
p-cscf 172.16.14.25;
session-timeout 0;
idle-timeout 0;
idle-timeout-direction both;
aaa-profile aaa-access-profile-1;
restriction-value 0;
address-assignment-method {
    aaa;
    inet-pool {
        pool pool-1;
    }
    charging {
        default-charging-profile default-charging-profile-apn-1;
    }
}
```

```
user@MBG1# show interfaces
mif {
    unit 0 {
        family inet;
    }
}
```

```
user@MBG1# show routing-instances User1-VRF interfaces
mif.0;
ge-0/0/0.5;
```

After you configure the device, enter **commit** from configuration mode.

## Verification

### Verifying the APN Configuration

---

<b>Purpose</b>	Verify that the APN is configured or not.
<b>Action</b>	From operational mode, enter the <b>show unified-edge ggsn-pgw apn statistics apn-name apn-1</b> command.
<b>Meaning</b>	The APN configured ( <b>apn-1</b> in this case) will display a number of statistics such as address allocation and user authentication statistics. Non-zero values in these fields are a sign that the APN is functioning.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Configuring Address Assignment on a Broadband Gateway APN on page 122</a></li><li>• <a href="#">Configuring APNs on the MobileNext Broadband Gateway Overview on page 113</a></li><li>• <a href="#">Configuring APN Service Selection on a Broadband Gateway on page 135</a></li><li>• <a href="#">Configuring Charging, Local Policy, and Policy and Charging Enforcement Function Profiles on a Broadband Gateway APN on page 131</a></li><li>• <a href="#">Configuring General APN Parameters on the Broadband Gateway on page 117</a></li><li>• <a href="#">Configuring Mobile Interfaces for APNs on page 133</a></li><li>• <a href="#">Configuring Mobile Interface to APN Associations in VRFs on page 134</a></li><li>• <a href="#">Configuring the Restriction Value on a Broadband Gateway APN on page 121</a></li><li>• <a href="#">Configuring User Options on a Broadband Gateway APN on page 141</a></li></ul>

## Networks Behind the Mobile Device Overview

---

The fundamental function of a MobileNext Broadband Gateway configured as a Gateway GPRS Support Node (GGSN) or Packet Data Network Gateway (P-GW) is to provide IP connectivity and services to the mobile subscriber. In small office, home office (SOHO) environments, the mobile user equipment can act as a router, connecting to more than one IP address associated with the user equipment. If some form of Network Address Translation (NAT) is not used in the mobile equipment, the IP address associated with this “mobile router” user equipment need not necessarily be associated with the addresses of the network (or networks) behind the mobile equipment.

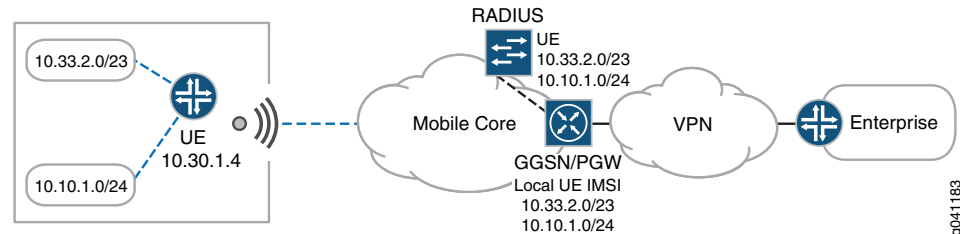
The broadband gateway supports typical use scenarios for networks behind the mobile equipment when the mobile device:

- Acts as a gateway for devices behind it, and these devices do not have 3G or 4G interfaces.
- Acts as a branch office customer edge (CE) router with a 3G or 4G interface to back up a primary fixed network link.



Figure 37 on page 147 shows that the IP prefixes for networks behind the mobile equipment (10.33.2.0/23 and 10.10.1.0/24) are not in the same IP address space as the mobile device itself (10.33.1.4). These addresses can be obtained locally or through a RADIUS server (both are shown in the figure).

**Figure 37: Network That Is Behind the Mobile Device and the P-GW**



The networks behind the mobile equipment feature is enabled at the access point name (APN) level. When a mobile subscriber establishes a session using the APN, the broadband gateway learns about the prefixes (networks) that are behind the mobile subscriber either through RADIUS (using the framed route attributes in the Access-Accept messages from the RADIUS server) or through the CLI configuration. The prefixes obtained from RADIUS take precedence over the local configuration.

These network-behind-mobile prefixes (routes) are advertised by routing protocols. The routes also populate the mobile subscriber database in the anchor packet forwarding engine and are associated with the appropriate mobile subscriber. This enables the anchor packet forwarding engine to forward the network-behind-mobile traffic using the GPRS tunneling protocol (GTP) tunnel associated with the mobile subscriber. Other subscriber-specific features such as charging and quality of service are applied to network-behind-mobile traffic.



**NOTE:** Routes from the authentication, authorization, and accounting (AAA) server override the prefixes configured for the APN.

#### Related Documentation

- [Configuring the Networks Behind the Mobile Equipment Feature on page 148](#)
- [Example: Configuring the Networks Behind the Mobile Device Feature on page 150](#)

## Configuring the Networks Behind the Mobile Equipment Feature

---

The MobileNext Broadband Gateway can support a network of devices behind the mobile device. You configure the addresses for network-behind-mobile devices by associating a list of IPv4 or IPv6 prefixes with an International Mobile Subscriber Identifier (IMSI) inside an access point name (APN). You can configure a limit to the number of IPv4 or IPv6 prefixes that the anchor Packet Forwarding Engine stores.

You can configure the networks behind the mobile equipment in one of the following general ways:

- Using RADIUS—You enable the networks behind the mobile equipment feature and obtain prefixes from the RADIUS server (you must configure RADIUS separately).
- Using local configuration—You enable the networks behind the mobile equipment feature and list the prefixes locally in the CLI.



**NOTE:** If you configure both RADIUS and local methods, then prefixes learned through RADIUS override those configured locally.

---

Before you begin configuring the networks behind the mobile equipment feature on a broadband gateway APN, you should have done the following:

- Configured the chassis of the broadband gateway
- Configured the interfaces of the broadband gateway
- Configured the APN parameters for the specific APN

You can associate up to 32 prefixes with a mobile device. If the user equipment sets up multiple sessions to the same APN, then the network-behind-mobile prefixes apply to only the first session.

To configure the networks behind the mobile equipment feature:

1. Enable the networks behind the mobile equipment feature for the APN called **nbm-apn**.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns nbm-apn]  
user@host# set allow-network-behind-mobile
```

**NOTE:**

- If you intend to obtain network-behind-mobile prefixes from the RADIUS server, this is the only step required. However, you must configure the RADIUS server based on the following information:
  - For IPv4 routes, the RADIUS server must be configured to send the Framed-Route attribute-value pair (AVP) as part of the Access Accept Response message to the broadband gateway.
  - For IPv6 routes, the RADIUS server must be configured to send the Framed-IPv6-Route AVP as part of the Access Accept Response message to the broadband gateway.
  - The format of the Framed-Route and Framed-IPv6-Route AVP is as follows: "*Host\_IPAddr*[/*SubnetMask*] *GW\_IPAddr* [*Metric*]", where:
    - *Host\_IPAddr*—IPv4 or IPv6 address of the destination host or network.
    - *SubnetMask*—(Optional) Subnet mask.
    - *GW\_IPAddr*—IP address of the broadband gateway.
    - *Metric*—(Optional) Metric (number of hops) for this route.

An example of a Framed-Route AVP is Framed-Route="192.168.1.0/24 192.168.1.1 1", and an example of a Framed-IPv6-Route AVP is Framed-IPv6-Route="2000:0:0:106::/64 2000::106:a00:20ff:fe99:a998 1".

- In addition, if you intend to assign an IP address to the user equipment using the RADIUS server, then you must configure the RADIUS server to return the Framed-IP-Address AVP or the Framed-IPv6-Prefix AVP for IPv4 and IPv6 addresses, respectively. For more information, see [“Configuring Address Assignment on a Broadband Gateway APN” on page 122](#).

2. For local network-behind-mobile prefixes, configure the **local** statement for address assignment for the APN called **nbm-apn**.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns nbm-apn]
user@host# set address-assignment local
```

3. For local network-behind-mobile prefixes, configure the **network-behind-mobile** statement for the APN called **nbm-apn**.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apn nbm-apn]
user@host# set network-behind-mobile
```

4. For local network-behind-mobile prefixes, configure the **imsi** statement and value of IPv4 or IPv6 prefixes associated with this mobile device.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apn nbm-apn
network-behind-mobile]
```

```
user@host# set imsi 111222330012347 prefix-v4 20.1.1.0/24 prefix-v6  
2003:2002:21::0/48
```



NOTE: You can configure up to 32 IPv4 or IPv6 prefixes.

5. (Optional) Configure the maximum number of network-behind-mobile IPv4 prefixes on the broadband gateway for each anchor Packet Forwarding Engine configured on the broadband gateway.

```
[edit unified-edge gateways ggsn-pgw MBG1]  
user@host# set anchor-pfe-ipv4-nbm-prefixes 16
```



NOTE: The limit is set in thousands from 16 to 128.

6. (Optional) Configure the maximum number of IPv6 prefixes on the broadband gateway for networks behind the mobile equipment of the anchor Packet Forwarding Engine.

```
[edit unified-edge gateways ggsn-pgw MBG1]  
user@host# set anchor-pfe-ipv6-nbm-prefixes 32
```



NOTE: The limit is set in thousands from 16 to 128.

#### Related Documentation

- [allow-network-behind-mobile](#)
- [anchor-pfe-ipv4-nbm-prefixes](#)
- [anchor-pfe-ipv6-nbm-prefixes](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 122](#)
- [Example: Configuring the Networks Behind the Mobile Device Feature on page 150](#)
- [network-behind-mobile](#)
- [Networks Behind the Mobile Device Overview on page 146](#)

---

## Example: Configuring the Networks Behind the Mobile Device Feature

This example shows how to configure the networks behind the mobile equipment feature for an access point name (APN) on the MobileNext Broadband Gateway. The APN assigns these addresses locally, but they can be overridden by an authentication, authorization, and accounting (AAA) server such as RADIUS. The APN, called **nbm-apn**, is configured on mobile interface 0 (**mif.0**).

- [Requirements on page 151](#)
- [Overview on page 152](#)
- [Configuration on page 152](#)
- [Verification on page 153](#)

## Requirements

This example uses the following hardware and software components:

- An MX Series chassis (except the MX80) equipped with session Dense Port Concentrators (DPCs) and interface Packet Forwarding Engines (housed in DPCs or Modular Port Concentrators [MPCs]).
- The Junos OS Mobility package software

Before you begin:

- Install the chassis hardware.
- Configure the chassis, as well as interfaces, anchors, and (optionally) redundancy.
- Configure RADIUS.



### NOTE:

- If you intend to obtain network-behind-mobile prefixes from the RADIUS server, this is the only step required. However, you must configure the RADIUS server based on the following information:
  - For IPv4 routes, the RADIUS server must be configured to send the Framed-Route attribute-value pair (AVP) as part of the Access Accept Response message to the broadband gateway.
  - For IPv6 routes, the RADIUS server must be configured to send the Framed-IPv6-Route AVP as part of the Access Accept Response message to the broadband gateway.
  - The format of the Framed-Route and Framed-IPv6-Route AVP is as follows: "*Host\_IPAddr*[/*SubnetMask*] *GW\_IPAddr* [*Metric*]", where:
    - *Host\_IPAddr*—IPv4 or IPv6 address of the destination host or network.
    - *SubnetMask*—(Optional) Subnet mask.
    - *GW\_IPAddr*—IP address of the broadband gateway.
    - *Metric*—(Optional) Metric (number of hops) for this route.

An example of a Framed-Route AVP is Framed-Route="192.168.1.0/24 192.168.1.1", and an example of a Framed-IPv6-Route AVP is Framed-IPv6-Route="2000:0:0:106::/64 2000::106:a00:20ff:fe99:a998 1".

- In addition, if you intend to assign an IP address to the user equipment using the RADIUS server, then you must configure the RADIUS server to return the Framed-IP-Address AVP or the Framed-IPv6-Prefix AVP for IPv4 and IPv6 addresses, respectively. For more information, see [“Configuring Address Assignment on a Broadband Gateway APN” on page 122](#).

## Overview

In this example, the broadband gateway has only one APN configured. Few APN parameters are configured in this example, which emphasizes the networks behind the mobile equipment feature. The mobile interface is configured (**mif.0**), and then the address assignment is done locally.

In detail, the broadband gateway is named **MBG1** and the APN is called **nbm-apn**. Most general APN parameters either use the default values or are not configured.

This configuration assigns the IPv4 prefixes **192.168.27.0/24** and **192.168.48.0/24** to a mobile device with the International Mobile Subscriber Identifier (IMSI) of **11222330012347**.

## Configuration

### CLI Quick Configuration

The networks behind the mobile equipment feature referenced above is configured by:

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns nbm-apn]
user@host# set mobile-interface mif.0
user@host# set allow-network-behind-mobile
user@host# set address-assignment local
user@host# set network-behind-mobile imsi 11222330012347 prefix-ipv4-list
192.168.27.0/24 192.168.48.0/24
```

### Step-by-Step Procedure

To configure the networks behind the mobile equipment feature:

1. Specify the mobile interface for the APN called **nbm-apn**.  

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns nbm-apn]
user@host# set mobile-interface mif.0
```
2. Enable the networks behind the mobile equipment feature.  

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns nbm-apn]
user@host# set allow-network-behind-mobile
```
3. Specify that the broadband gateway assigns addresses locally to subscribers, using the mobile pool or mobile pool group configured for the APN.  

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns nbm-apn]
user@host# set address-assignment local
```
4. For local network-behind-mobile prefixes, configure the IMSI of the user equipment and the IPv4 prefixes associated with the user equipment.  

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns nbm-apn]
user@host# set network-behind-mobile imsi 11222330012347 prefix-ipv4-list
192.168.27.0/24 192.168.48.0/24
```

### Results

From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, these **show** command outputs include only the configuration that is relevant to this example.

```

user@host# show unified-edge gateways ggsn-pgw MBG1 apn-services apns nbm-apn
allow-network-behind-mobile;
mobile-interface mif.0;
address-assignment-method {
    local;
}
network-behind-mobile {
    imsi 111222330012347 {
        192.168.27.0/24;
        192.168.48.0/24;
    }
}

```

After you configure the device, enter **commit** in configuration mode to commit your changes.

## Verification

### Verifying the Networks Behind the Mobile Equipment Configuration

<b>Purpose</b>	Verify that a mobile subscriber is associated with the configured network-behind-mobile prefixes.
<b>Action</b>	From operational mode, enter the <b>show unified-edge ggsn-pgw gateway MBG1 subscribers extensive</b> command.
<b>Meaning</b>	The output associated with the IMSI (111222330012347 in this case) displays a list of IPv4 addresses as <b>IPv4 NBM address</b> (although the prefixes are listed for the APN <b>nbm-apn</b> ).
<b>Related Documentation</b>	<ul style="list-style-type: none"> <li>• <i>allow-network-behind-mobile</i></li> <li>• <a href="#">Configuring Address Assignment on a Broadband Gateway APN on page 122</a></li> <li>• <a href="#">Configuring the Networks Behind the Mobile Equipment Feature on page 148</a></li> <li>• <i>network-behind-mobile</i></li> <li>• <a href="#">Networks Behind the Mobile Device Overview on page 146</a></li> </ul>

## HTTP Header Enrichment Overview

Mobile subscribers accessing Web-based services often need to have content added to the Hypertext Transport Protocol (HTTP) headers sent back and forth as part of the client-server exchange. This HTTP header enrichment is a feature that can be configured on the MobileNext Broadband Gateway for an Access Point Name (APN).

HTTP header enrichment adds information such as the Mobile Subscriber ISDN (MS-ISDN) number to HTTP headers.

For example, this feature can add the last line to this sequence of HTTP headers:

```

GET /256k.html HTTP/1.1
Host: 10.45.45.2

```

```
Accept */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; NET CLR 1.1.4322
name: value
X-MSISDN: <MSISDN #>
```

You configure HTTP header enrichment by installing one or more Multiservices Dense Port Concentrators (MS-DPCs) in the broadband gateway chassis, and configuring and applying a service set to the mobile interface for the configured APN. This feature maintains statistics for the flows to which it is applied.

- Related Documentation**
- [Configuring HTTP Header Enrichment on page 154](#)
  - [Example: Configuring HTTP Header Enrichment on page 157](#)

---

## Configuring HTTP Header Enrichment

The MobileNext Broadband Gateway can support content added to the Hypertext Transport Protocol (HTTP) headers sent back and forth as part of the client-server exchange for mobile subscribers accessing Web-based services. You configure HTTP header enrichment as a service for an access point name (APN).

Before you begin configuring HTTP header enrichment for a broadband gateway APN, you should have done the following:

- Configured the chassis of the broadband gateway
- Configured the interfaces of the broadband gateway
- Configured the Packet Data Network Gateway (P-GW) parameters for the broadband gateway
- Configured the APN parameters for the specific APN

You must make sure that the **JUNOS Services HTTP Content Management package** and **JUNOS Services Mobile Subscriber Service Container package** are installed on the device. Use the **show version** command to provide a list of installed services.

If the HTTP header enrichment interface configured is in the form **amsn**, then per-subscriber load-balancing is performed. If the HTTP header enrichment interface configured is in the form **msn**, then no load balancing (or redundancy) is performed. In either case, the **interface** statement at the **system** hierarchy level of the PGW is required for all subscriber-aware services because the subscriber is anchored on the service PIC interface.



To configure HTTP header enrichment for an APN, you implement and apply a typical services set and rule with **from** and **then** clauses:



**NOTE:** You can configure more than one match condition in the **from** clause, and more than one action in the **then** clause, but you must configure at least one for each.

1. Configure the **destination-address** statement at the **hcm** hierarchy level to define the IP address to which to apply the HTTP header extension information. In this step, the **destination-address** statement is configured as a **from** clause inside a term called **1** inside a **tag-rule** called **rule1**.



**NOTE:** The **term** argument must have a numeric value.

```
[edit services hcm tag-rule rule1 term 1 from]
user@host# set destination-address any-unicast
```

2. Configure the **destination-address-range** and specify a low-to-high IP address range for the header enrichment.

```
[edit services hcm tag-rule rule1 term 1 from]
user@host# set destination-address-range low 10.10.10.1 high 10.10.10.255/32
```

3. Configure the **destination-port** number for the header extension.

```
[edit services hcm tag-rule rule1 term 1 from]
user@host# set destination-port 1004
```

4. Configure the **destination-port-range** number and specify a low-to-high port range for the header enrichment.

```
[edit services hcm tag-rule rule1 term 1 from]
user@host# set destination-port-range low 1000 high 2000
```

5. Configure the **destination-prefix-list** to reference a predefined prefix list for the header enrichment.

```
[edit services hcm tag-rule rule1 term 1 from]
user@host# set destination-prefix-list hcm-prefix-list
```

6. Configure the **tag-header** statement at the **hcm** hierarchy level to determine the tag header to apply to the HTTP header. In this step, the **tag-header** statement is configured under a **tag** statement named **msisdn** inside a **then** clause inside **1** of the **tag-rule** called **rule1**.

```
[edit services hcm tag-rule rule1 term 1 then tag msisdn]
user@host# set tag-header X_MSISDN
```

7. Configure the **tag-attribute** statement at the **hcm** hierarchy level to determine the list tag attributes to apply to the HTTP header.

```
[edit services hcm]
user@host# set tag-attribute msisdn
```



**NOTE:** The tag attribute must be listed to be used in the tag rule.

8. Configure the **tag-attribute** statement at the **hcm** hierarchy level to determine the tag attribute to apply to the HTTP header. In this step, the **tag-attribute** statement is configured under a **tag** statement named *msisdn* inside a **then** clause inside *1* of the **tag-rule** called *rule1*.

```
[edit services hcm tag-rule rule1 term 1 then tag msisdn]
user@host# set tag-attribute msisdn
```



**NOTE:** The tag attribute must be listed in the tag attributes established at the **hcm** hierarchy level.

9. Configure the **tag-separator** statement to specify a separator to use for header enrichment.

```
[edit services hcm tag-rule rule1 term 1 then tag msisdn]
user@host# set tag-separator ,
```

10. Configure the **encrypt** statement to specify a hash method and prefix key to use for header enrichment.

```
[edit services hcm tag-rule rule1 term 1 then tag msisdn]
user@host# set encrypt md5 prefix gatewaykey1
```

11. If you have more than one tag rule, create a tag rule set to group multiple configured rules.

```
[edit services hcm tag-rule-set rule-set-1]
user@host# set tag-rule rule1
user@host# set tag-rule rule2
```

12. Apply the tag rule or the tag rule set to a service set. This step applies a single tag rule named *rule1*.

```
[edit services service-set service-set-1]
user@host# set tag-rules rule1
```

13. Include the **subscriber-awareness** statement as a service set option for the mobile service set.

```
[edit services service-set service-set-1 service-set-options]
user@host# set subscriber-awareness
```

14. Include the **resource-triggered** statement as a load-balancing hash key option for the mobile service interface.

```
[edit services service-set service-set-1 interface-service service-interface ams1.1
load-balancing-options hash-keys]
user@host# set resource-triggered
```

15. Apply the service set to the mobile interface for the APN for input and output.

```
[edit interfaces mif unit 0 family inet service]
user@host# set input service-set service-set-1
user@host# set output service-set service-set-1
```

16. Include the **interface** statement gateway system configuration.

```
[edit unified-edge gateways ggsn-pgw MBG1 system]
user@host# set anchor-service-pics interface ams0
```



**NOTE:** This statement is required for all subscriber-aware services because the subscriber is anchored on the service PIC interface.

17. Include the **jservice-hcm** and **jservices-mss** packages with the services PIC configuration.

```
[edit chassis fpc 3 pic 0 adaptive-services service-package extension-provider]
user@host# set package jservices-hcm
user@host# set package jservices-mss
```

- Related Documentation**
- [HTTP Header Enrichment Overview on page 153](#)
  - [Example: Configuring HTTP Header Enrichment on page 157](#)

## Example: Configuring HTTP Header Enrichment

This example shows how to configure the HTTP header enrichment service on an Access Point Name (APN) on the MobileNext Broadband Gateway. The example shows not only the configuration of the service set and **hcm** stanza, but all other CLI pieces required to successfully enable this service.

- [Requirements on page 157](#)
- [Overview on page 157](#)
- [Configuration on page 158](#)
- [Verification on page 163](#)

### Requirements

This example uses the following hardware and software components:

- An MX240, MX480, or MX960 running the MobileNext software
- Junos OS Release 11.4W or later

Before you begin:

- Configure the chassis, along with redundancy and anchors.
- Configure the Packet Data Network Gateway (P-GW).
- Configure the APN and APN interfaces.

### Overview

This example adds a Mobile Subscriber ISDN (MS-ISDN) and International Mobile Subscriber Number (IMSI) field to the HTTP headers on all unicast destination addresses

for traffic flowing through the APN (**APN1**) on the P-GW (**MBG1**). The APN is configured to use the mobile interface **mif.0**, and the services PIC used is PIC 0 on FPC 3. The HTTP header enrichment interface configured is in the form **amsn** so that per-subscriber load balancing is performed.

## Configuration

### CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the commands into the CLI at the **[edit]** hierarchy level.



**NOTE:** This example assumes several rule, APN, and interface names, as well as other variables. If your variables are different, you must change these details.

```
set services hcm tag-rule rule1 term 1 from destination-address any-unicast
set services hcm tag-rule rule1 term 1 then tag msisdn
set services hcm tag-rule rule1 term 1 then tag msisdn tag-header msisdn
set services hcm tag-rule rule1 term 1 then tag-attribute msisdn
set services hcm tag-rule rule1 term 1 then tag imsi
set services hcm tag-rule rule1 term 1 then tag imsis tag-header imsi
set services hcm tag-rule rule1 term 1 then tag-attribute imsi

set services service-set service-set-1 tag-rules rules1
set services service-set service-set-1 interface-service service-interface ams1.1
set services service-set service-set-1 tag-rules rules1 load-balancing-options hash-keys
resource-triggered

set interfaces mif unit 0 family inet service input service-set-1
set interfaces mif unit 0 family inet service output service-set-1

set unified-edge gateways ggsn-pgw MBG1 system anchor-services-pics interface ams0

set chassis fpc 3 pic 0 adaptive-services service-package extension-provider package
jservices-hcm
set chassis fpc 3 pic 0 adaptive-services service-package extension-provider package
jservices-mss
```



**NOTE:** Make sure you apply these statements to the correct hardware and software components.

**Step-by-Step  
Procedure**

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see “*Using the CLI Editor in Configuration Mode*” in the *Junos OS CLI User Guide*.

To configure HTTP header enrichment to add the MS-ISDN and IMSI to the HTTP header for any unicast destination address:

1. Configure the **destination-address** statement at the **hcm** hierarchy level to define the IP address to which to apply the HTTP header extension information. In this step, the **destination-address** statement is configured as a **from** clause inside a term called **1** inside a **tag-rule** called **rule1**.

```
[edit services hcm tag-rule rule1 term 1 from]
user@host# set destination-address 10.10.10.1/32
```

2. Configure the **tag-header** statement at the **hcm** hierarchy level to determine the tag header to apply to the HTTP header. In this step, the **tag-header** statement is configured under a **tag** statement named **msisdn** inside a **then** clause inside **1** of the **tag-rule** called **rule1**.

```
[edit services hcm tag-rule rule1 term 1 then tag msisdn]
user@host# set tag-header X_MSISDN
```

3. Configure the **tag-attribute** statement at the **hcm** hierarchy level to determine the list tag attributes to apply to the HTTP header.

```
[edit services hcm]
user@host# set tag-attribute msisdn imsi
```



**NOTE:** The tag attribute must be listed to be used in the tag rule.

4. Configure the **tag-attribute** statement at the **hcm** hierarchy level to determine the MS-ISDN tag attribute to apply to the HTTP header. In this step, the **tag-attribute** statement is configured under a **tag** statement named **msisdn** inside a **then** clause inside **1** of the **tag-rule** called **rule1**.

```
[edit services hcm tag-rule rule1 term 1 then tag msisdn]
user@host# set tag-attribute msisdn
```



**NOTE:** The tag attribute must be listed in the tag attributes established at the **hcm** hierarchy level.

5. Configure the **tag-attribute** statement at the **hcm** hierarchy level to determine the IMSI tag attribute to apply to the HTTP header. In this step, the **tag-attribute** statement is configured under a **tag** statement named **imsi** inside a **then** clause inside **1** of the **tag-rule** called **rule1**.

```
[edit services hcm tag-rule rule1 term 1 then tag msisdn]
user@host# set tag-attribute imsi
```



**NOTE:** The tag attribute must be listed in the tag attributes established at the **hcm** hierarchy level.

6. Apply the tag rule or the tag rule set to a service set. This step applies a single tag rule named *rule1*.

```
[edit services service-set service-set-1]
user@host# set tag-rules rule1
```

7. Include the **subscriber-awareness** statement as a service set option for the mobile service set.

```
[edit services service-set service-set-1 service-set-options]
user@host# set subscriber-awareness
```

8. include the **resource-triggered** statement as a load-balancing hash key option for the mobile service interface.

```
[edit services service-set service-set-1 interface-service service-interface ams1.1
load-balancing-options hash-keys]
user@host# set resource-triggered
```

9. Apply the service set to the mobile interface for the APN for input and output.

```
[edit interfaces mif unit 0 family inet service]
user@host# set input service-set service-set-1
user@host# set output service-set service-set-1
```

10. Include the **interface** statement for the P-GW.

```
[edit unified-edge gateways ggsn-pgw MBG1 system]
user@host# set anchor-service-pics interface ams0
```

11. Include the **jservice-hcm** and **jservices-mss** packages with the services PIC configuration.

```
[edit chassis fpc 3 pic 0 adaptive-services service-package extension-provider]
user@host# set package jservices-hcm
user@host# set package jservices-mss
```

12. Include the recommended aggregated multiservices PIC (**ams**) configuration for per-subscriber load balancing.

```
[edit interfaces ams0 load-balancing-options member-failure-options]
user@host# set redistribute-all-traffic enable-rejoin
user@host# set drop-member-traffic rejoin-timeout 10
```



**NOTE:** Although you can configure an *ms-* interface, we recommend load balancing with an *ams-* interface for HTTP header enrichment.

**Results** From configuration mode, confirm your configuration by entering the **show** command at the proper hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, these **show** command outputs include only the configuration that is relevant to this example. Any other configuration on the system is replaced with ellipses (...).

```
(...)
services {
  service-set services-set-1 {
    service-set-options {
      subscriber-awareness;
    }
    tag-rules rule1;
    interface-service {
      service-interface ams1.1;
      load-balancing-options {
        hash-keys {
          resource-triggered;
        }
      }
    }
  }
}
hcm {
  tag-rule rule1 {
    term 1 {
      from {
        destination-address {
          any-unicast;
        }
      }
      then {
        tag msisdn {
          tag-header X-MSISDN;
          tag-attribute msisdn;
        }
        tag imsi {
          tag-header X-IMSI;
          tag-attribute imsi;
        }
      }
    }
  }
  tag-attribute [ msisdn imsi];
}
}
(...)
interfaces mif {
  unit 0 {
    family inet {
      service {
        input {
          service-set services-set-1;
        }
        output {
          service-set services-set-1;
        }
      }
    }
  }
}
```

```
    }
  }
  (...)
  unified-edge gateways ggsn-pgw MBG1 system {
    anchor-services-pics {
      interface ams1;
    }
  }
  unified-edge gateways ggsn-pgw MBG1 apn-services {
    apns {
      APN1 {
        mobile-interface mif.0;
        (...)
      }
    }
  }
  (...)
  chassis fpc 3 pic 0 {
    adaptive-services {
      service-package {
        extension-provider {
          control-cores 1;
          data-cores 6;
          object-cache-size 2560;
          policy-db-size 64;
          package jservices-hcm;
          package jservices-mss;
          package jservices-crypto-base;
        }
      }
    }
  }
  (...)
  interfaces ams0 {
    load-balancing-options {
      redistribute-all-traffic {
        enable-rejoin;
      }
      drop-member-traffic {
        rejoin-timeout 10;
      }
    }
  }
}
```





**NOTE:** Although you can configure HTTP header enrichment to use a non-load-balancing *ms-* service interface, we recommend configuring an *ams-* interface with load-balancing options used for HTTP header enrichment, as shown in this example. The `redistribute-all-traffic` statement removes the aggregated member from the traffic distribution list so that traffic is redistributed among active members, which affects the flow on all members of the group. The `drop-member-traffic` statement (with a high `rejoin-timeout` value) discards the traffic for a failed member until the rejoin timeout period expires. If the member recovers before this timeout period has expired, flows are again directed to the recovered member. If the member has not recovered in the timeout period, the failed member is removed from the group. Therefore, a high rejoin timeout minimizes the impact on existing members. HTTP header enrichment uses redundancy properties, but not hashing.

If you are done configuring the device, enter **commit** from configuration mode.

## Verification

### Verifying HTTP Header Enrichment

**Purpose** Verify whether HTTP header enrichment is enabled or not.

**Action** From operational mode, enter the **show services hcm statistics rule rule1** command.

**Meaning**

```

user@host: show services hcm statistics rule rule1
Interface: mams-3/1/0
Term id      Hits
1             58
Interface: mams-4/1/0
Term id      Hits
1            144
  
```

A non-zero value in the field **Hits** shows that the interfaces that are part of **ams1.1** are successfully performing HTTP header enrichment.

**Related Documentation**

- [HTTP Header Enrichment Overview on page 153](#)
- [Configuring HTTP Header Enrichment on page 154](#)



## PART 4

# Authorization, Addressing, and IPv6 Configuration

- [AAA Overview on page 167](#)
- [Configuring AAA on page 199](#)
- [Configuring Address Assignment on page 229](#)
- [Configuring DHCP on page 235](#)
- [Configuring IPv6 Stateless Address Autoconfiguration Parameters on page 247](#)



## CHAPTER 8

# AAA Overview

- [Overview of AAA on the Broadband Gateway on page 167](#)
- [Scalability and Redundancy on page 170](#)
- [Network Elements on page 171](#)
- [Network Element Groups on page 172](#)
- [AAA Profiles on page 172](#)
- [Supported Attributes in Access-Request Messages on page 174](#)
- [Supported Attributes in Access-Accept Messages on page 179](#)
- [Supported Attributes in Accounting Start Messages on page 182](#)
- [Supported Attributes in Accounting Interim Update Messages on page 186](#)
- [Supported Attributes in Accounting Stop Messages on page 190](#)
- [Supported Attributes in Accounting On Messages on page 195](#)
- [Supported Attributes in Disconnect Request Messages on page 196](#)
- [Supported Attributes in Change of Authorization \(CoA\) Messages on page 197](#)

## Overview of AAA on the Broadband Gateway

---

The MobileNext Broadband Gateway supports a framework for providing authentication, authorization, and accounting (AAA) services to mobile subscribers. The broadband gateway provides authentication (verifying a subscriber's username and password), authorization (receiving information about the types of services to deliver to the subscriber), and accounting (accumulating and providing statistics about services delivered to the subscriber) using groups of external RADIUS servers.

### Authentication

The broadband gateway acts as a client to the RADIUS server when authenticating a mobile subscriber's username and password. When the broadband gateway receives a Create PDP Context Request or Create Session Request message from a mobile subscriber, it gets the subscriber's authentication information from the message, then sends an Access-Request message to the RADIUS server. The Access-Request message contains attributes such as the subscriber username, password, the ID of the client, and the port ID that the subscriber is accessing.

Once the RADIUS server receives the Access-Request message, it validates the sending client (the broadband gateway) using a shared secret. After the sending client is validated, the RADIUS server looks up the subscriber in its database. A list of requirements must be met to allow access for the subscriber. If any requirement is not met, the RADIUS server sends an Access-Reject message back to the broadband gateway, indicating that the subscriber's access request is invalid.

If the requirements are met, a list of configuration values for the subscriber is placed into an Access-Accept message response. These values include the types of services for which the subscriber is authorized, as well as all necessary values to deliver the services.

To determine a subscriber's username, the broadband gateway looks at the Protocol Configuration Options (PCO) received in the Create PDP Context Request or Create Session Request message. If the subscriber's username is included in the PCO, then that is used for authentication. If the subscriber's username cannot be determined from the PCO or if the **override-pco** statement is configured, then the username specified in the **user-options** configuration for the access point name (APN) is used instead. The username can be an actual username that you configure, the APN name, the subscriber's International Mobile Subscriber Identity (IMSI), or the subscriber's Mobile Station Integrated Services Digital Network (MSISDN) number.

To determine the subscriber's password, the broadband gateway does the following:

- For the Password Authentication Protocol (PAP), the broadband gateway looks for the password in the PCO of the Create PDP Context Request or Create Session Request message. If the password cannot be determined from the PCO or if the **override-pco** statement is configured, the password specified in the **user-options** configuration for the APN is used instead.
- For the Challenge Handshake Authentication Protocol (CHAP), type, length, and values (TLVs) for the CHAP challenge and CHAP password (concatenation of CHAP ID and CHAP password) both arrive in the PCO. The broadband gateway includes these TLVs in the Access-Request message sent to the RADIUS server.

If the RADIUS server responds with an Access-Challenge or Access-Reject message, or if no response is received from the RADIUS server, the broadband gateway does not create a session for the subscriber.

## Accounting

A PDP context configured to use RADIUS accounting causes the broadband gateway to generate an Accounting Start message at the start of service delivery. The broadband gateway sends that message to the RADIUS accounting server, which sends back an acknowledgement that the message has been received. The Accounting Start message contains RADIUS attributes describing the type of service being delivered and the subscriber to which it is being delivered. Subscriber passwords are not carried in accounting messages.

At the end of service delivery, the broadband gateway generates an Accounting Stop message describing the type of service that was delivered and statistics such as elapsed time, input/output octets, and input/output packets. It sends that message to the RADIUS

accounting server, which sends back an acknowledgement that the message has been received.

During the life of a user session, some information related to the session may change. Upon reception of an Update PDP Context Request message from the Serving GPRS Support Node (SGSN), or upon reception of a Modify Bearer Request or Update Bearer Response from the Serving Gateway (S-GW), the broadband gateway sends an Accounting Request Interim-Update message to the RADIUS server to update information related to this PDP context. You can configure how often Interim-Update messages are sent, and specify which events do or do not trigger them.

## APN-Specific AAA Settings

AAA services are provided on a per-APN basis. Mobile subscribers gaining access to a given APN receive AAA services as indicated in a defined AAA profile. The AAA profile specifies which sets of RADIUS servers are used for authentication and accounting, how the broadband gateway handles attributes in RADIUS messages it sends and receives, as well as other parameters. You specify the name of the AAA profile to use as part of APN services configuration.

In the APN services configuration, you can also configure the broadband gateway to allow the RADIUS server to assign addresses to mobile subscribers, override the locally or DHCP-assigned address with a RADIUS-assigned address, or wait for the accounting response from the RADIUS server before sending the Create Session Response or Create PDP Context Response message to the S-GW or SGSN.

## RADIUS-Initiated Dynamic Requests

You can specify RADIUS servers that can initiate dynamic requests to the broadband gateway. Dynamic requests include change of authorization (CoA) requests, which specify attribute modifications and service changes, and Disconnect requests, which terminate subscriber sessions.

- See [“Supported Attributes in Change of Authorization \(CoA\) Messages” on page 197](#) for information about RADIUS attributes and Third-Generation Partnership Project (3GPP) vendor-specific attributes (VSAs) supported in CoA requests.
- See [“Supported Attributes in Disconnect Request Messages” on page 196](#) for information about RADIUS attributes and 3GPP VSAs supported in Disconnect requests.

## Support for RADIUS Attributes, Juniper Networks VSAs, and 3GPP VSAs

The AAA framework on the broadband gateway supports RADIUS attributes and VSAs from Juniper Networks and the 3GPP. The tables in [“Supported Attributes in Access-Request Messages” on page 174](#) and [“Supported Attributes in Access-Accept Messages” on page 179](#) describe how the broadband gateway processes these attributes and VSAs.

### Related Documentation

- [Configuring APNs on the MobileNext Broadband Gateway Overview on page 113](#)
- [Configuring AAA on the Broadband Gateway on page 199](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 122](#)

- [Configuring User Options on a Broadband Gateway APN on page 141](#)
- [Example: Configuring AAA on the Broadband Gateway on page 213](#)

## Scalability and Redundancy

---

To accommodate the substantial amount of authentication, authorization, and accounting (AAA) traffic that can be generated in a 3G/4G mobile network, the AAA implementation on the MobileNext Broadband Gateway is optimized for scalability and redundancy, both in the way the broadband gateway distributes AAA functions to its services PICs, and in the way it sends requests to the external RADIUS servers.

### Scalability

Each session DPC installed on the broadband gateway contains two services PICs. Each services PIC runs a separate AAA instance, which serves as a Network Access Server (NAS) for mobile subscriber sessions. When a mobile subscriber session requires AAA services, its anchor Modular Port Concentrator (MPC) assigns one of the services PICs to handle interaction with the RADIUS servers for the duration of that session. By installing additional session DPCs, you can increase the number of services PICs providing NAS functionality, and thus increase the number of sessions for which the broadband gateway can provide AAA services.

Rather than use a single RADIUS server for authentication or accounting, the broadband gateway sends RADIUS requests to a load-balanced group of RADIUS servers called a *network element*. To broadcast accounting traffic to multiple network elements, you can configure *network element groups*, consisting of from one to four network elements. The broadband gateway sends accounting messages to one of the network elements in the group, or can broadcast them to all of the network elements in the group.

### Redundancy

Services PICs can be configured in redundant pairs, with one services PIC active and the other standby. In this kind of configuration, the active services PIC synchronizes its pending requests with the backup services PIC. When a switchover occurs, any pending requests are then sent from the new active services PIC.

The broadband gateway can detect when RADIUS servers in a network element have failed. When the broadband gateway detects a dead server, it automatically starts sending RADIUS requests to a different server in the network element. You can set a priority level for individual RADIUS servers in the network element, so that the AAA traffic fails over to a selected server.

#### Related Documentation

- [MobileNext Broadband Gateway Chassis Overview on page 68](#)
- [Broadband Gateway Redundancy Overview on page 78](#)
- [Network Elements on page 171](#)
- [Network Element Groups on page 172](#)



---

## Network Elements

---

A network element is a load-balanced group of RADIUS servers that provides authentication, authorization, and accounting (AAA) services for mobile subscribers accessing an access point name (APN).

When a mobile subscriber attempts to get access to an APN, the broadband gateway sends an Access-Request message to one of the RADIUS servers in the network element the APN is configured to use for authentication. Similarly, accounting messages for the mobile subscriber go to the network element the APN is configured to use for accounting.

Network elements for authentication and accounting are specified in the AAA profile that is applied to the APN.

### Load Balancing Within Network Elements

To facilitate the large number of mobile subscriber sessions requiring AAA services, the broadband gateway distributes the RADIUS messages across the servers in the network element, using one of the following load-balancing algorithms:

- Direct (default)—Causes all requests to go to the first server listed in the network element configuration; if that server cannot handle additional requests, they go to the next server in the list.
- Round-robin—Sends the first request to the first server listed in the network element configuration, the second request to the second server in the list, and so on.

### Server Priority

Within a network element, a RADIUS server can be assigned a priority of 1 or 2. The broadband gateway distributes RADIUS messages only to the priority 1 servers, using the configured load-balancing algorithm. If all the priority 1 servers should fail, then the broadband gateway starts using the priority 2 servers.

### Dead Server Detection

To determine whether a RADIUS server in a network element has failed, the broadband gateway keeps track of how often requests sent to a server time out and must be retransmitted. If requests need to be retransmitted a given number of times over a given interval, the broadband gateway marks the server as “dead,” then starts sending requests to the next available server in the network element (to a priority 1 server if one is available, or a priority 2 server if no priority 1 servers are available).

At the same time, the broadband gateway starts a timer (the *revert-interval*) for the server. After this timer expires, the broadband gateway marks the dead server alive again, and once again includes it in the rotation for sending RADIUS messages.

### Maximum Pending Requests for a Network Element

You can specify the maximum number of requests that can be queued to the network element. When the pending request queue is full, any additional requests are dropped.

If the number of pending requests reaches 80 percent of the maximum, an SNMP trap is generated.

**Related  
Documentation**

- [AAA Profiles on page 172](#)
- [Configuring Network Elements on page 203](#)
- [Network Element Groups on page 172](#)

---

## Network Element Groups

A network element group is a list of between one and four network elements to which the MobileNext Broadband Gateway sends accounting messages.

You can configure the following options for a network element group:

- **mandatory**—Indicates that a response is mandatory from a specified network element before any services can be provided to the subscriber.
- **broadcast**—Broadcasts the accounting messages to all network elements in the group.

When the **broadcast** parameter is configured, the accounting requests are sent to all of the network elements in the network element group. Note that when the **broadcast** parameter is configured, at least one of the network elements in the group must be configured with the **mandatory** parameter. If the **broadcast** parameter is not specified, then the broadband gateway sends the accounting requests to the first network element in the group. If there is no response, then it tries the next network element in the group, and so on.

**Related  
Documentation**

- [AAA Profiles on page 172](#)
- [Configuring Network Elements on page 203](#)
- [Configuring Network Element Groups on page 204](#)

---

## AAA Profiles

An authentication, authorization, and accounting (AAA) profile is a collection of authentication, accounting, and RADIUS attribute settings that can be applied to an access point name (APN). When mobile subscribers access the APN to which an AAA profile is applied, they receive authentication and accounting services as specified in the AAA profile.

The following sections describe the settings that can be configured in an AAA profile.

### Authentication Options

In the AAA profile, you specify a network element (load-balanced RADIUS server group) to be used for authenticating mobile subscribers.

## Accounting Options

In an AAA profile, you can specify the following options for RADIUS accounting:

- The name of the network element or network element group to use for RADIUS accounting.
- Whether the broadband gateway sends an Accounting-On message when a services PIC is restarted.
- How often the broadband gateway sends Interim-Update messages for accounting. The broadband gateway can send Interim-Update messages at specified intervals and when specific trigger events occur.

By default, the broadband gateway sends Interim-Update messages for the following trigger events:

- The IPv4 address update for the mobile subscriber is deferred.
- The Mobile Station (MS) time zone changes.
- The Public Land Mobile Network (PLMN) to which the mobile subscriber is attached changes.
- The quality of service (QoS) profile applied by the broadband gateway for the Packet Data Protocol (PDP) context or Evolved Packet System (EPS) bearer changes.
- The Radio Access Technology (RAT) serving the mobile subscriber changes.
- The SGSN/S-GW serving the mobile subscriber changes.
- The location information for the mobile subscriber changes.

You can optionally disable sending of Interim Update messages for any of these trigger events.

## RADIUS Attributes to Ignore or Exclude

The AAA profile can specify which RADIUS attributes the broadband gateway ignores in Access-Accept messages it receives, as well as which RADIUS attributes the broadband gateway excludes from specific types of RADIUS messages it generates.

## RADIUS Options

In an AAA profile, you can set the following options for RADIUS attributes:

- NAS-IP-Address (RADIUS attribute 4)

This attribute specifies the IP address of the network access server (NAS) that is requesting authentication for the mobile subscriber. By default, this attribute contains the IP address configured for the RADIUS **source-interface** statement. When you specify a value for the `nas-ip-address` option in the AAA profile, the broadband gateway uses this IP address as the value for the NAS-IP-Address attribute in RADIUS requests.

- Prefix for NAS-Identifier (RADIUS attribute 32)

The NAS-Identifier attribute is a string that identifies the NAS that originated the Access-Request message for the AAA session. On the broadband gateway, the anchor Modular Port Concentrator (MPC) selects a services PIC to handle AAA operations for the duration of the session. The services PIC functions as the NAS for the AAA session.

Specifying a value for the nas-identifier-prefix option in the AAA profile configures the broadband gateway to include the NAS-Identifier attribute in RADIUS requests. In this case, the broadband gateway appends the ID of the services PIC to the value specified for the nas-identifier-prefix option, and uses the combined prefix and services PIC ID as the value for the NAS-Identifier attribute. If the services PICs are part of a redundancy group, the broadband gateway appends the aggregated multiservices interface (ams) ID to the prefix instead of the services PIC ID.

- NAS-Port-Type (RADIUS Attribute 61)

This attribute indicates the type of port used for authenticating the mobile subscriber. In an AAA profile, you can specify a port type of *virtual* or *wireless* for the nas-port-type option. If you specify a value for the nas-port-type option, the broadband gateway uses this as the value for the NAS-Port-Type attribute in RADIUS requests.

**Related  
Documentation**

- [Configuring an AAA Profile on page 204](#)
- [Configuring Network Elements on page 203](#)
- [Configuring Network Element Groups on page 204](#)

---

## Supported Attributes in Access-Request Messages

The following tables indicate how the MobileNext Broadband Gateway processes RADIUS attributes and 3GPP VSAs in RADIUS Access-Request messages. An Access-Request message is sent by the broadband gateway to the RADIUS server to convey username, password, and other information to be used when authenticating a user.

- [RADIUS IETF Attributes Supported in Access-Request Messages on page 174](#)
- [3GPP VSAs Supported in Access-Request Messages on page 176](#)

### RADIUS IETF Attributes Supported in Access-Request Messages

[Table 16 on page 175](#) lists the RADIUS attributes supported by the broadband gateway in Access-Request messages.

Table 16: RADIUS IETF Attributes Supported in Access-Request Messages

Attribute Number	Attribute Name	Description	Content
1	User-Name	<p>The username is provided to the broadband gateway by the user in the Protocol Configuration Options (PCO) received during the IP-CAN session establishment procedure.</p> <p>If no username is available, then the username configured in the <b>user-options</b> statement of the APN configuration is used instead. If the <b>override-pco</b> statement is configured, then the gateway overrides the username and password obtained from the PCO PAP or CHAP in the Create PDP Context Request or Create Session Request message with the username and password configured for the APN.</p>	String
2	User-Password	<p>If Password Authentication Protocol (PAP) is used, the user password is provided to the broadband gateway by the user in the PCO received during the IP-CAN session establishment procedure.</p> <p>If no user password is available, then the password specified in the <b>user-options</b> statement of the APN configuration is used instead.</p>	String
3	CHAP-Password	If Challenge Handshake Authentication Protocol (CHAP) is used, the password provided by the user (extracted from the PCO field of the Create PDP Context Request message).	String (can have two contiguous, with 0x00 in between)
4	NAS-IP-Address	IPv4 address of the broadband gateway for communication with the RADIUS server.	IPv4 address
6	Service-Type	Type of service the user has requested or the type of service to be provided.	2 (Framed)
7	Framed-Protocol	Type of protocol for the user.	7 (GPRS PDP context)
8	Framed-IP-Address	IPv4 address allocated for this user.	IPv4 address
9	Framed-IP-Netmask	Network mask allocated for this user's IP address.	IPv4 netmask

**Table 16: RADIUS IETF Attributes Supported in Access-Request Messages (*continued*)**

Attribute Number	Attribute Name	Description	Content
30	Called-Station-Id	Identifier for the target network (APN).	APN (UTF-8 encoded characters)
31	Calling-Station-ID	Identifier for the mobile station (MS), configurable on a per-APN basis.	MSISDN in international format, UTF-8 encoded decimal characters
32	NAS-Identifier	Identifier of the NAS originating the request, may be configured as a user-specified prefix and the ID of the services PIC handling NAS functions for the session.	String
44	Acct-Session-ID	User Session identifier, unique for every bearer under the session.	Broadband gateway Gn IP address (IPv4 or IPv6) and Charging-ID, concatenated in a UTF-8-encoded hexadecimal value
60	CHAP-Challenge	The CHAP Challenge is provided to the broadband gateway by the user in the PCO received during the IP-CAN session establishment procedure.	String
61	NAS-Port-Type	Type of physical port the broadband gateway is using to authenticate the user, may be configured on the broadband gateway as virtual or wireless.	Integer value indicating the port type (wireless or virtual) as specified in RFC 2865
97	Framed-IPv6-Prefix	IPv6 prefix that is configured for the user, can be used as a hint by the NAS to the RADIUS server that it would prefer this prefix.	Value indicating the prefix, as specified in RFC 3162

### 3GPP VSAs Supported in Access-Request Messages

[Table 17 on page 176](#) lists the 3GPP vendor-specific attributes (VSAs) supported by the broadband gateway in Access-Request messages.

**Table 17: 3GPP VSAs Supported in Access-Request Messages**

Attribute Number	Attribute Name	Description	Content
26/10415/1 (3GPP type 1)	3GPP-IMSI	IMSI for this user.	UTF-8 encoded string
26/10415/2	3GPP-Charging-Id	Charging ID for this PDP context/EPS bearer.	Integer

Table 17: 3GPP VSAs Supported in Access-Request Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
26/10415/3	3GPP-PDP Type	<p>For a GGSN, this indicates the type of PDP context; for example, IP or PPP.</p> <p>For a P-GW, this indicates the PDN type: IPv4, IPv6, or IPv4v6.</p>	Integer
26/10415/4	3GPP-CG-Address	Charging gateway IP address.	IPv4 address, or 0.0.0.0 if no charging gateway is configured on the broadband gateway.
26/10415/5	3GPP-GPRS-Negotiated-QoS-Profile	QoS profile applied by the broadband gateway for the PDP context/EPS bearer.	UTF-8 encoded string
26/10415/6	3GPP-SGSN-Address	<p>For a GGSN, this represents the SGSN IPv4 address that is used by the GTP control plane for the handling of control messages.</p> <p>For a P-GW, this represents the IPv4 address of the S-GW, trusted non-3GPP IP access, or ePDG that is used on S5/S8, S2a, or S2b for the handling of control messages.</p> <p>This attribute may be used to identify the PLMN to which the user is attached.</p>	IPv4 address
26/10415/7	3GPP-GGSN-Address	<p>For a GGSN, this represents the GGSN IPv4 address that is used by the GTP control plane for the context establishment.</p> <p>For a P-GW, this represents the P-GW IPv4 address that is used on the S5/S8, S2a, S2b, or S2c control plane for the IP-CAN session establishment.</p> <p>The address is the same as the GGSN/P-GW IPv4 address used in the CDRs generated by the broadband gateway.</p>	IPv4 address
26/10415/8	3GPP-IMSI-MCC-MNC	The MCC and MNC extracted from the user's IMSI (first 5 or 6 digits, as applicable from the presented IMSI).	String
26/10415/9	3GPP-GGSN-MCC-MNC	The MCC and MNC of the network to which the broadband gateway belongs.	String

Table 17: 3GPP VSAs Supported in Access-Request Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
26/10415/10	3GPP-NSAPI	Identifier for a particular PDP context for the associated PDN and MSISDN/IMSI, from creation to deletion.  For a P-GW, this identifies the EPS bearer ID if it is known to the P-GW.	String
26/10415/12	3GPP-Selection-Mode	Selection mode for this PDP context/EPS bearer, received in the Create PDP Context/Session Request message.	String
26/10415/13	3GPP-Charging-Characteristics	For a GGSN, this contains the charging characteristics for this PDP context, received in the Create PDP Context Request message (only available in R99 and later releases).  For a P-GW, this contains the charging characteristics for the IP-CAN bearer.	String
26/10415/18	3GPP-SGSN-MCC-MNC	The MCC and MNC extracted from the RAI from the Create PDP Context Request and Update PDP Context Request messages.	String
26/10415/20	3GPP-IMEISV	International Mobile Station Equipment Identity and Software Version Number (IMEISV).	String (UTF-8 encoded characters)
26/10415/21	3GPP-RAT-Type	The Radio Access Technology type that is currently serving the user equipment.	Octet string
26/10415/22	3GPP-User-Location-Info	Information about where the user equipment is currently located (for example, SAI or CGI).	Octet string
26/10415/23	3GPP-MS-TimeZone	The offset between UTC and local time in steps of 15 minutes of where the MS currently resides.	Octet string
26/10415/26	3GPP-Negotiated-DSCP	DSCP used to mark the IP packets of this PDP context on the Gi interface, or EPS bearer context on the SGi interface.	Octet string



Table 17: 3GPP VSAs Supported in Access-Request Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
26/10415/27	3GPP-Allocate-IP-Type	Indicates whether the Access-Request message is sent for user authentication only, or for allocation of IPv4 or IPv6 addresses, or both.	Octet string

- Related Documentation**
- [AAA Profiles on page 172](#)
  - [Configuring RADIUS Attribute Usage for an AAA Profile on page 207](#)
  - [Overview of AAA on the Broadband Gateway on page 167](#)
  - [Supported Attributes in Access-Accept Messages on page 179](#)

## Supported Attributes in Access-Accept Messages

The following tables indicate how the MobileNext Broadband Gateway processes RADIUS attributes or 3GPP and Juniper Networks VSAs received in RADIUS Access-Accept messages. If authentication is successful, the RADIUS server sends an Access-Accept message that provides specific configuration information necessary to begin delivery of service to the user.

- [RADIUS IETF Attributes Supported in Access-Accept Messages on page 179](#)
- [3GPP VSAs Supported in Access-Accept Messages on page 181](#)
- [Juniper Networks VSAs Supported in Access-Accept Messages on page 181](#)

## RADIUS IETF Attributes Supported in Access-Accept Messages

Table 18 on page 179 lists the RADIUS attributes supported by the broadband gateway in Access-Accept messages.

Table 18: RADIUS IETF Attributes Supported in Access-Accept Messages

Attribute Number	Attribute Name	Description	Content
1	User-Name	The username received in the Access-Request message, or a substitute username provided by the RADIUS server.  If a value for the User-Name attribute is received in the Access-Accept message, it takes precedence over any other value for the username.	String
6	Service-Type	Type of service the user has requested or the type of service to be provided.	Value indicating the service type, as specified in RFC 2865

Table 18: RADIUS IETF Attributes Supported in Access-Accept Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
7	Framed-Protocol	Type of protocol for the user.	Value indicating the protocol, as specified in RFC 2865
8	Framed-IP-Address	IPv4 address allocated for this user, if the RADIUS server is used to allocate IP addresses.	IPv4 address
9	Framed-IP-Netmask	Network mask allocated for this user's IP address, if applicable.	IPv4 netmask
25	Class	Unmodified identifier to be used in all subsequent accounting messages.	String
27	Session-Timeout	Maximum number of seconds of service to be provided to the user before termination of the session or prompt.	32-bit unsigned integer
28	Idle-Timeout	Maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt.	32-bit unsigned integer
85	Acct-Interim-Interval	Number of seconds between each accounting interim update to be sent from the NAS for this session.	Integer
88	Framed-Pool	Name of an assigned address pool to be used to assign an address for the user.	String
96	Framed-Interface-Id	IPv6 interface identifier to be configured for the user.	8-octet ID
97	Framed-IPv6-Prefix	IPv6 prefix and corresponding route to be configured for the user.	Value indicating the prefix, as specified in RFC 3162
100	Framed-IPv6-Pool	Name of the assigned pool to be used to assign an IPv6 prefix for the user.	String
123	Delegated-IPv6-Prefix	IPv6 prefix to be used.	Value indicating the prefix, as specified in RFC 4818
26/311	MS- primary-DNS-server	Primary DNS server address for this APN.	IPv4 address
26/311	MS-Secondary-DNS-Server	Secondary DNS server address for this APN.	IPv4 address

Table 18: RADIUS IETF Attributes Supported in Access-Accept Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
26/311	MS-Primary-NBNS-Server	Primary NetBios name server address for this APN.	IPv4 address
26/311	MS-Secondary-NBNS-Server	Secondary NetBios name server address for this APN.	IPv4 address

### 3GPP VSAs Supported in Access-Accept Messages

Table 20 on page 181 lists the 3GPP vendor-specific attributes (VSAs) supported by the broadband gateway in Access-Accept messages.

Table 19: 3GPP VSAs Supported in Access-Accept Messages

Attribute Number	Attribute Name	Description	Content
26/10415/5	3GPP-GPRS-Negotiated-QoS-Profile	QoS profile applied by the broadband gateway for the PDP context/EPS bearer.	UTF-8 encoded string
26/10415/13	3GPP-Charging-Characteristics	For a GGSN, this contains the charging characteristics for this PDP context, received in the Create PDP Context Request message (only available in R99 and later releases).  For a P-GW, this contains the charging characteristics for the IP-CAN bearer.	String
26/10415/17	3GPP-IPv6-DNS-Servers	List of IPv6 addresses of DNS servers for this APN.	IPv6 addresses

### Juniper Networks VSAs Supported in Access-Accept Messages

Table 20 on page 181 lists the Juniper Networks VSAs supported by the broadband gateway in Access-Accept messages. The AAA framework uses vendor ID 4874, which is assigned to Juniper Networks by the Internet Assigned Numbers Authority (IANA).

Table 20: Juniper VSAs Supported in Access-Accept Messages

Attribute Number	Attribute Name	Description	Content
26/4874/2	Local-Address-Pool	Name of the IP address pool configured on the broadband gateway to be used for address allocation for this PDP context.	String
26/4874/175	Redirect-Gw-Addr	Address of the gateway to which the user session should be redirected.	IPv4 address
26/4874/176	APN-Name	Name of the APN.	String

- Related Documentation**
- [AAA Profiles on page 172](#)
  - [Configuring RADIUS Attribute Usage for an AAA Profile on page 207](#)
  - [Overview of AAA on the Broadband Gateway on page 167](#)
  - [Supported Attributes in Access-Request Messages on page 174](#)

## Supported Attributes in Accounting Start Messages

The following tables indicate how the MobileNext Broadband Gateway processes RADIUS attributes and 3GPP VSAs in RADIUS Accounting Start messages. An Accounting Start message indicates to the RADIUS server that the user session has started, and specifies quality of service (QoS) parameters associated with the session.

- [RADIUS IETF Attributes Supported in Accounting Start Messages on page 182](#)
- [3GPP VSAs Supported in Accounting Start Messages on page 183](#)

### RADIUS IETF Attributes Supported in Accounting Start Messages

Table 21 on page 182 lists the RADIUS attributes supported by the broadband gateway in Accounting Start messages.

**Table 21: RADIUS IETF Attributes Supported in Accounting Start Messages**

Attribute Number	Attribute Name	Description	Content
1	User-Name	<p>The username provided to the broadband gateway by the user in the Protocol Configuration Options (PCO) received during the IP-CAN session establishment procedure.</p> <p>If no username is available, then the username configured in the <b>user-options</b> statement of the APN configuration is used instead. If the <b>override-pco</b> statement is configured, then the gateway overrides the username and password obtained from the PCO PAP or CHAP in the Create PDP Context Request or Create Session Request message with the username and password configured for the APN.</p> <p>If a value for the User-Name attribute was received in the Access-Accept message, it takes precedence over any other value for the username.</p>	String
4	NAS-IP-Address	IPv4 address of the broadband gateway for communication with the RADIUS server.	IPv4 address

Table 21: RADIUS IETF Attributes Supported in Accounting Start Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
6	Service-Type	Type of service the user has requested or the type of service to be provided.	Value indicating the service type, as specified in RFC 2865
7	Framed-Protocol	Type of protocol for the user.	Value indicating the protocol, as specified in RFC 2865
25	Class	Unmodified identifier received in the Access-Accept message.	String
30	Called-Station-Id	Identifier for the target network (APN).	APN (UTF-8 encoded characters)
31	Calling-Station-ID	Identifier for the mobile station (MS), configurable on a per-APN basis.	MSISDN in international format, UTF-8 encoded decimal characters
32	NAS-Identifier	Identifier of the NAS originating the request.	String
40	Acct-Status-Type	Type of accounting message.	Integer
41	Acct-Delay-Time	Number of seconds the broadband gateway has been trying to send this accounting record.	32-bit unsigned integer
44	Acct-Session-ID	User Session identifier, unique for every bearer under the session.	Broadband gateway Gn IP address (IPv4 or IPv6) and Charging-ID, concatenated in a UTF-8-encoded hexadecimal value
45	Acct-Authentic	Method by which user was authenticated: whether by RADIUS, the NAS itself, or another remote authentication protocol.	1 - RADIUS 2 - Local 3 - Remote
55	Event-Timestamp	Time that this event occurred on the NAS, in seconds, since January 1, 1970 00:00 UTC.	32-bit unsigned integer
61	NAS-Port-Type	Type of physical port the broadband gateway is using to authenticate the user, may be configured on the broadband gateway as virtual or wireless.	Value indicating the port type, as specified in RFC 2865

### 3GPP VSAs Supported in Accounting Start Messages

Table 22 on page 184 lists the 3GPP vendor-specific attributes (VSAs) supported by the broadband gateway in Accounting Start messages.

Table 22: 3GPP VSAs Supported in Accounting Start Messages

Attribute Number	Attribute Name	Description	Content
26/10415/1 (3GPP type 1)	3GPP-IMSI	IMSI for this user.	String
26/10415/2	3GPP-Charging-Id	Charging ID for this PDP context/EPS bearer.	String
26/10415/3	3GPP-PDP Type	For a GGSN, this indicates the type of PDP context; for example, IP or PPP.  For a P-GW, this indicates the PDN type: IPv4, IPv6, or IPv4v6.	String
26/10415/5	3GPP-GPRS-Negotiated-QoS-Profile	QoS profile applied by the broadband gateway for the PDP context/EPS bearer.	UTF-8 encoded string
26/10415/6	3GPP-SGSN-Address	For a GGSN, this represents the SGSN IPv4 address that is used by the GTP control plane for the handling of control messages.  For a P-GW, this represents the IPv4 address of the S-GW, trusted non-3GPP IP access, or ePDG that is used on S5/S8, S2a, or S2b for the handling of control messages.  This attribute may be used to identify the PLMN to which the user is attached.	IPv4 address
26/10415/7	3GPP-GGSN-Address	For a GGSN, this represents the GGSN IPv4 address that is used by the GTP control plane for the context establishment.  For a P-GW, this represents the P-GW IPv4 address that is used on the S5/S8, S2a, S2b, or S2c control plane for the IP-CAN session establishment.  The address is the same as the GGSN/P-GW IPv4 address used in the CDRs generated by the broadband gateway.	IPv4 address
26/10415/8	3GPP-IMSI-MCC-MNC	The MCC and MNC extracted from the user's IMSI (first 5 or 6 digits, as applicable from the presented IMSI).	String

Table 22: 3GPP VSAs Supported in Accounting Start Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
26/10415/9	3GPP-GGSN-MCC-MNC	The MCC and MNC of the network to which the broadband gateway belongs.	String
26/10415/10	3GPP-NSAPI	Identifier for a particular PDP context for the associated PDN and MSISDN/IMSI, from creation to deletion.  For a P-GW, this identifies the EPS bearer ID if it is known to the P-GW.	String
26/10415/12	3GPP-Selection-Mode	Selection mode for this PDP context/EPS bearer, received in the Create PDP Context/Session Request message.	String
26/10415/13	3GPP-Charging-Characteristics	For a GGSN, this contains the charging characteristics for this PDP context, received in the Create PDP Context Request message (only available in R99 and later releases).  For a P-GW, this contains the charging characteristics for the IP-CAN bearer.	String
26/10415/18	3GPP-SGSN-MCC-MNC	The MCC and MNC extracted from the RAI from the Create PDP Context Request and Update PDP Context Request messages.	String
26/10415/20	3GPP-IMEISV	International Mobile Station Equipment Identity and Software Version Number (IMEISV).	String (UTF-8 encoded characters)
26/10415/21	3GPP-RAT-Type	The Radio Access Technology type that is currently serving the user equipment.	Integer
26/10415/22	3GPP-User-Location-Info	Information about where the user equipment is currently located (for example, SAI or CGI).	Octet string
26/10415/23	3GPP-MS-TimeZone	The offset between UTC and local time in steps of 15 minutes of where the MS currently resides.	Octet string

- Related Documentation**
- [AAA Profiles on page 172](#)
  - [Configuring RADIUS Attribute Usage for an AAA Profile on page 207](#)
  - [Overview of AAA on the Broadband Gateway on page 167](#)

- [Supported Attributes in Accounting Interim Update Messages on page 186](#)
- [Supported Attributes in Accounting On Messages on page 195](#)
- [Supported Attributes in Accounting Stop Messages on page 190](#)

## Supported Attributes in Accounting Interim Update Messages

The following tables indicate how the MobileNext Broadband Gateway processes RADIUS attributes and 3GPP VSAs in RADIUS accounting Interim-Update messages. An accounting Interim-Update message is sent by the broadband gateway when it receives an Update PDP Context Request message from the SGSN. It is used to update information related to the PDP context.

- [RADIUS IETF Attributes Supported in Interim-Update Messages on page 186](#)
- [3GPP VSAs Supported in Interim-Update Messages on page 188](#)

### RADIUS IETF Attributes Supported in Interim-Update Messages

Table 23 on page 186 lists the RADIUS attributes supported by the broadband gateway in Interim-Update messages.

Table 23: RADIUS IETF Attributes Supported in Accounting Interim-Update Messages

Attribute Number	Attribute Name	Description	Content
1	User-Name	<p>The username provided to the broadband gateway by the user in the Protocol Configuration Options (PCO) received during the IP-CAN session establishment procedure.</p> <p>If no username is available, then the username configured in the <b>user-options</b> statement of the APN configuration is used instead. If the <b>override-pco</b> statement is configured, then the gateway overrides the username and password obtained from the PCO PAP or CHAP in the Create PDP Context Request or Create Session Request message with the username and password configured for the APN.</p> <p>If a value for the User-Name attribute was received in the Access-Accept message, it takes precedence over any other value for the username.</p>	String
4	NAS-IP-Address	IPv4 address of the broadband gateway for communication with the RADIUS server.	IPv4 address



**Table 23: RADIUS IETF Attributes Supported in Accounting Interim-Update Messages (*continued*)**

Attribute Number	Attribute Name	Description	Content
6	Service-Type	Type of service the user has requested or the type of service to be provided.	Value indicating the service type, as specified in RFC 2865
7	Framed-Protocol	Type of protocol for the user.	Value indicating the protocol, as specified in RFC 2865
25	Class	Unmodified identifier received in the Access-Accept message.	String
30	Called-Station-Id	Identifier for the target network (APN).	APN (UTF-8 encoded characters)
31	Calling-Station-ID	Identifier for the mobile station (MS), configurable on a per-APN basis.	MSISDN in international format, UTF-8 encoded decimal characters
32	NAS-Identifier	Identifier of the NAS originating the request.	String
40	Acct-Status-Type	Type of accounting message.	Integer
41	Acct-Delay-Time	Number of seconds the broadband gateway has been trying to send this accounting record.	32-bit unsigned integer
42	Acct-Input-Octets	Number of octets sent by the user for the IP-CAN bearer.	32-bit unsigned integer
43	Acct-Output-Octets	Number of octets received by the user for the IP-CAN bearer.	32-bit unsigned integer
44	Acct-Session-ID	User Session identifier, unique for every bearer under the session.	Broadband gateway Gn IP address (IPv4 or IPv6) and Charging-ID, concatenated in a UTF-8-encoded hexadecimal value
45	Acct-Authentic	Method by which the user was authenticated: whether by RADIUS, the NAS itself, or another remote authentication protocol.	Integer: 1 - RADIUS 2 - Local 3 - Remote
46	Acct-Session-Time	Duration of the session, in seconds.	Integer
47	Acct-Input-Packets	Number of packets sent by the user.	Integer
48	Acct-Output-Packets	Number of packets received by the user.	Integer

**Table 23: RADIUS IETF Attributes Supported in Accounting Interim-Update Messages (continued)**

Attribute Number	Attribute Name	Description	Content
52	Acct-Input-Gigawords	How many times the Acct-Input-Octets counter has wrapped around $2^{32}$ over the course of this PDP session.	32-bit unsigned integer
53	Acct-Output-Gigawords	How many times the Acct-Output-Octets counter has wrapped around $2^{32}$ over the course of this PDP session.	32-bit unsigned integer
55	Event-Timestamp	Time that this event occurred on the NAS, in seconds, since January 1, 1970 00:00 UTC.	32-bit unsigned integer
123	Delegated-IPv6-Prefix	IPv6 prefix to be used.	Value indicating the prefix, as specified in RFC 4818

### 3GPP VSAs Supported in Interim-Update Messages

Table 24 on page 188 lists the 3GPP vendor-specific attributes (VSAs) supported by the broadband gateway in Interim-Update messages.

**Table 24: 3GPP VSAs Supported in Accounting Interim-Update Messages**

Attribute Number	Attribute Name	Description	Content
26/10415/1 (3GPP type 1)	3GPP-IMSI	IMSI for this user.	String
26/10415/2	3GPP-Charging-Id	Charging ID for this PDP context or EPS bearer.	String
26/10415/3	3GPP-PDP Type	For a GGSN, this indicates the type of PDP context; for example, IP or PPP.  For a P-GW, this indicates the PDN type: IPv4, IPv6, or IPv4v6.	String
26/10415/4	3GPP-CG-Address	Charging gateway IP address.	IPv4 address, or 0.0.0.0 if no charging gateway is configured on the broadband gateway
26/10415/5	3GPP-GPRS-Negotiated-QoS-Profile	QoS profile applied by the broadband gateway for the PDP context or EPS bearer.	UTF-8 encoded string

Table 24: 3GPP VSAs Supported in Accounting Interim-Update Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
26/10415/6	3GPP-SGSN-Address	<p>For a GGSN, this represents the SGSN IPv4 address that is used by the GTP control plane for the handling of control messages.</p> <p>For a P-GW, this represents the IPv4 address of the S-GW, trusted non-3GPP IP access, or ePDG that is used on S5/S8, S2a, or S2b for the handling of control messages.</p> <p>This attribute may be used to identify the PLMN to which the user is attached.</p>	IPv4 address
26/10415/7	3GPP-GGSN-Address	<p>For a GGSN, this represents the GGSN IPv4 address that is used by the GTP control plane for the context establishment.</p> <p>For a P-GW, this represents the P-GW IPv4 address that is used on the S5/S8, S2a, S2b, or S2c control plane for the IP-CAN session establishment.</p> <p>The address is the same as the GGSN/P-GW IPv4 address used in the CDRs generated by the broadband gateway.</p>	IPv4 address
26/10415/8	3GPP-IMSI-MCC-MNC	The MCC and MNC extracted from the user's IMSI (first 5 or 6 digits, as applicable from the presented IMSI).	String
26/10415/9	3GPP-GGSN-MCC-MNC	The MCC and MNC of the network to which the broadband gateway belongs.	String
26/10415/10	3GPP-NSAPI	<p>Identifier for a particular PDP context for the associated PDN and MSISDN/IMSI, from creation to deletion.</p> <p>For a P-GW, this identifies the EPS bearer ID if it is known to the P-GW.</p>	String
26/10415/12	3GPP-Selection-Mode	Selection mode for this PDP context or EPS bearer, received in the Create PDP Context/Session Request message.	String
26/10415/13	3GPP-Charging-Characteristics	<p>For a GGSN, this contains the charging characteristics for this PDP context, received in the Create PDP Context Request message (only available in R99 and later releases).</p> <p>For a P-GW, this contains the charging characteristics for the IP-CAN bearer.</p>	String

Table 24: 3GPP VSAs Supported in Accounting Interim-Update Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
26/10415/18	3GPP-SGSN-MCC-MNC	The MCC and MNC extracted from the RAI from the Create PDP Context Request and Update PDP Context Request messages.	String
26/10415/21	3GPP-RAT-Type	The Radio Access Technology type that is currently serving the user equipment.	Integer
26/10415/22	3GPP-User-Location-Info	Information about where the user equipment is currently located (for example, SAI or CGI).	Octet string
26/10415/23	3GPP-MS-TimeZone	The offset between UTC and local time in steps of 15 minutes of where the MS currently resides.	Octet string

**Related Documentation**

- [AAA Profiles on page 172](#)
- [Configuring RADIUS Attribute Usage for an AAA Profile on page 207](#)
- [Overview of AAA on the Broadband Gateway on page 167](#)
- [Supported Attributes in Accounting On Messages on page 195](#)
- [Supported Attributes in Accounting Start Messages on page 182](#)
- [Supported Attributes in Accounting Stop Messages on page 190](#)

## Supported Attributes in Accounting Stop Messages

The following tables indicate how the MobileNext Broadband Gateway processes RADIUS attributes and 3GPP VSAs in RADIUS Accounting Stop messages. An Accounting Stop message is sent by the broadband gateway when it receives a Delete PDP Context Request message (provided a RADIUS Accounting Start message had been sent previously). It indicates the termination of this particular user session.

- [RADIUS IETF Attributes Supported in Accounting Stop Messages on page 190](#)
- [3GPP VSAs Supported in Accounting Stop Messages on page 193](#)

### RADIUS IETF Attributes Supported in Accounting Stop Messages

[Table 25 on page 191](#) lists the RADIUS attributes supported by the broadband gateway in Accounting Stop messages.

Table 25: RADIUS IETF Attributes Supported in Accounting Stop Messages

Attribute Number	Attribute Name	Description	Content
1	User-Name	<p>The username provided to the broadband gateway by the user in the Protocol Configuration Options (PCO) received during the IP-CAN session establishment procedure.</p> <p>If no username is available, then the username configured in the <b>user-options</b> statement of the APN configuration is used instead. If the <b>override-pco</b> statement is configured, then the gateway overrides the username and password obtained from the PCO PAP or CHAP in the Create PDP Context Request or Create Session Request message with the username and password configured for the APN.</p> <p>If a value for the User-Name attribute was received in the Access-Accept message, it takes precedence over any other value for the username.</p>	String
4	NAS-IP-Address	IPv4 address of the broadband gateway for communication with the RADIUS server.	IPv4 address
6	Service-Type	Type of service the user has requested or the type of service to be provided.	Value indicating the service type, as specified in RFC 2865
7	Framed-Protocol	Type of protocol for the user.	Value indicating the protocol, as specified in RFC 2865
25	Class	Unmodified identifier received in the Access-Accept message.	String
30	Called-Station-Id	Identifier for the target network (APN).	APN (UTF-8 encoded characters)
31	Calling-Station-ID	Identifier for the mobile station (MS), configurable on a per-APN basis.	MSISDN in international format, UTF-8 encoded decimal characters.
32	NAS-Identifier	Identifier of the NAS originating the request.	String
40	Acct-Status-Type	Type of accounting message.	Integer
41	Acct-Delay-Time	Number of seconds the broadband gateway has been trying to send this accounting record.	32-bit unsigned integer

Table 25: RADIUS IETF Attributes Supported in Accounting Stop Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
42	Acct-Input-Octets	Number of octets sent by the user for the IP-CAN bearer.	32-bit unsigned integer
43	Acct-Output-Octets	Number of octets received by the user for the IP-CAN bearer.	32-bit unsigned integer
44	Acct-Session-ID	User Session identifier, unique for every bearer under the session.	Broadband gateway Gn IP address (IPv4 or IPv6) and Charging-ID, concatenated in a UTF-8-encoded hexadecimal value
45	Acct-Authentic	Method by which user was authenticated: whether by RADIUS, the NAS itself, or another remote authentication protocol.	Integer: 1 - RADIUS 2 - Local 3 - Remote
46	Acct-Session-Time	Duration of the session, in seconds.	Integer
47	Acct-Input-Packets	Number of packets sent by the user.	Integer
48	Acct-Output-Packets	Number of packets received by the user.	Integer
49	Acct-Terminate-Cause	Reason the session was terminated. The session can be terminated for the following reasons: <ul style="list-style-type: none"> <li>• User Request (1)—User initiated the disconnect (log out).</li> <li>• NAS Error (9)—Negotiation failures, connection failures, or address lease expiration.</li> <li>• NAS Request (10)—PPP challenge timeout, PPP request timeout, tunnel establishment failure, PPP bundle failure, IP address lease expiration, PPP keep-alive failure, tunnel disconnect, or an unaccounted-for error.</li> </ul>	Integer
52	Acct-Input-Gigawords	How many times the Acct-Input-Octets counter has wrapped around $2^{32}$ over the course of this PDP session.	32-bit unsigned integer
53	Acct-Output-Gigawords	How many times the Acct-Output-Octets counter has wrapped around $2^{32}$ over the course of this PDP session.	32-bit unsigned integer

Table 25: RADIUS IETF Attributes Supported in Accounting Stop Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
55	Event-Timestamp	Time that this event occurred on the NAS, in seconds, since January 1, 1970 00:00 UTC.	32-bit unsigned integer

### 3GPP VSAs Supported in Accounting Stop Messages

Table 26 on page 193 lists the 3GPP vendor-specific attributes (VSAs) supported by the broadband gateway in Accounting Stop messages.

Table 26: 3GPP VSAs Supported in Accounting Stop Messages

Attribute Number	Attribute Name	Description	Content
26/10415/1 (3GPP type 1)	3GPP-IMSI	IMSI for this user.	UTF-8 encoded string
26/10415/2	3GPP-Charging-Id	Charging ID for this PDP context/EPS bearer.	Integer
26/10415/3	3GPP-PDP Type	For a GGSN, this indicates the type of PDP context; for example, IP or PPP.  For a P-GW, this indicates the PDN type: IPv4, IPv6, or IPv4v6.	Integer
26/10415/5	3GPP-GPRS-Negotiated-QoS-Profile	QoS profile applied by the broadband gateway for the PDP context/EPS bearer.	UTF-8 encoded string
26/10415/6	3GPP-SGSN-Address	For a GGSN, this represents the SGSN IPv4 address that is used by the GTP control plane for the handling of control messages.  For a P-GW, this represents the IPv4 address of the S-GW, trusted non-3GPP IP access or ePDG that is used on S5/S8, S2a or S2b for the handling of control messages.  This attribute may be used to identify the PLMN to which the user is attached.	IPv4 address

Table 26: 3GPP VSAs Supported in Accounting Stop Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
26/10415/7	3GPP-GGSN-Address	<p>For a GGSN, this represents the GGSN IPv4 address that is used by the GTP control plane for the context establishment.</p> <p>For a P-GW, this represents the P-GW IPv4 address that is used on the S5/S8, S2a, S2b or S2c control plane for the IP-CAN session establishment.</p> <p>The address is the same as the GGSN/P-GW IPv4 address used in the CDRs generated by the broadband gateway.</p>	IPv4 address
26/10415/8	3GPP-IMSI-MCC-MNC	The MCC and MNC extracted from the user's IMSI (first 5 or 6 digits, as applicable from the presented IMSI).	String
26/10415/9	3GPP-GGSN-MCC-MNC	The MCC and MNC of the network to which the broadband gateway belongs.	String
26/10415/10	3GPP-NSAPI	<p>Identifier for a particular PDP context for the associated PDN and MSISDN/IMSI, from creation to deletion.</p> <p>For a P-GW, this identifies the EPS bearer ID if it is known to the P-GW.</p>	String
26/10415/12	3GPP-Selection-Mode	Selection mode for this PDP context/EPS bearer, received in the Create PDP Context/Session Request message.	String
26/10415/13	3GPP-Charging-Characteristics	<p>For a GGSN, this contains the charging characteristics for this PDP context, received in the Create PDP Context Request message (only available in R99 and later releases).</p> <p>For a P-GW, this contains the charging characteristics for the IP-CAN bearer.</p>	String
26/10415/18	3GPP-SGSN-MCC-MNC	The MCC and MNC extracted from the RAI from the Create PDP Context Request and Update PDP Context Request messages.	String
26/10415/21	3GPP-RAT-Type	The Radio Access Technology type that is currently serving the user equipment.	Octet string
26/10415/22	3GPP-User-Location-Info	Information about where the user equipment is currently located (for example, SAI or CGI).	Octet string



Table 26: 3GPP VSAs Supported in Accounting Stop Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
26/10415/23	3GPP-MS-TimeZone	The offset between UTC and local time in steps of 15 minutes of where the MS currently resides.	Octet string

**Related Documentation**

- [AAA Profiles on page 172](#)
- [Configuring RADIUS Attribute Usage for an AAA Profile on page 207](#)
- [Overview of AAA on the Broadband Gateway on page 167](#)
- [Supported Attributes in Accounting Interim Update Messages on page 186](#)
- [Supported Attributes in Accounting On Messages on page 195](#)
- [Supported Attributes in Accounting Start Messages on page 182](#)

## Supported Attributes in Accounting On Messages

The following table lists the RADIUS attributes supported by the MobileNext Broadband Gateway in RADIUS Accounting On messages. Accounting On messages are sent by the broadband gateway to the RADIUS server to ensure correct synchronization of session information.

- [RADIUS IETF Attributes Supported in Accounting On Messages on page 195](#)

## RADIUS IETF Attributes Supported in Accounting On Messages

[Table 27 on page 195](#) lists the RADIUS attributes supported by the broadband gateway in Accounting On messages.

Table 27: RADIUS IETF Attributes Supported in Accounting On Messages

Attribute Number	Attribute Name	Description	Content
4	NAS-IP-Address	IPv4 address of the broadband gateway for communication with the RADIUS server.	IPv4 address
32	NAS-Identifier	Identifier of the NAS originating the request.	String
40	Acct-Status-Type	Type of accounting message.	Accounting-ON
41	Acct-Delay-Time	Number of seconds the broadband gateway has been trying to send this accounting record.	32-bit unsigned integer

**Related Documentation**

- [AAA Profiles on page 172](#)
- [Configuring RADIUS Attribute Usage for an AAA Profile on page 207](#)

- [Overview of AAA on the Broadband Gateway on page 167](#)
- [Supported Attributes in Accounting Interim Update Messages on page 186](#)
- [Supported Attributes in Accounting Start Messages on page 182](#)
- [Supported Attributes in Accounting Stop Messages on page 190](#)

## Supported Attributes in Disconnect Request Messages

The following tables list the RADIUS attributes and 3GPP VSAs supported by the MobileNext Broadband Gateway in RADIUS Disconnect Request messages. A Disconnect Request message is sent by the RADIUS server to terminate a user session on a NAS and discard all associated session contexts.

The broadband gateway listens on UDP ports 1700 and 3799 for RADIUS Disconnect Request messages sent from the RADIUS server. The user session identified by the Disconnect Request message is deleted on the broadband gateway.

- [RADIUS IETF Attributes Supported in Disconnect Request Messages on page 196](#)
- [3GPP VSAs Supported in Disconnect Request Messages on page 196](#)

### RADIUS IETF Attributes Supported in Disconnect Request Messages

[Table 28 on page 196](#) lists the RADIUS attributes supported by the broadband gateway in Disconnect Request messages.

**Table 28: RADIUS IETF Attributes Supported in Disconnect Request Messages**

Attribute Number	Attribute Name	Description	Content
1	User-Name	<p>The username received in the Access-Request message, or a substitute username provided by the RADIUS server.</p> <p>If a value for the User-Name attribute is received in the Access-Accept message, it takes precedence over any other value for the username.</p>	String
44	Acct-Session-ID	<p>User Session identifier, unique for every bearer under the session.</p> <p>The broadband gateway deletes the user session indicated by this attribute.</p>	Broadband gateway Gn IP address (IPv4 or IPv6) and Charging-ID, concatenated in a UTF-8-encoded hexadecimal value

### 3GPP VSAs Supported in Disconnect Request Messages

[Table 29 on page 197](#) lists the 3GPP VSAs supported by the broadband gateway in Disconnect Request messages.

Table 29: 3GPP VSAs Supported in Disconnect Request Messages

Attribute Number	Attribute Name	Description	Content
26/10415/1 (3GPP type 1)	3GPP-IMSI	IMSI for this user.	UTF-8 encoded string
26/10415/10	3GPP-NSAPI	Identifier for a particular PDP context for the associated PDN and MSISDN/IMSI, from creation to deletion.  For a P-GW, this identifies the EPS bearer ID if it is known to the P-GW.	String

- Related Documentation**
- [AAA Profiles on page 172](#)
  - [Configuring RADIUS Attribute Usage for an AAA Profile on page 207](#)
  - [Overview of AAA on the Broadband Gateway on page 167](#)

## Supported Attributes in Change of Authorization (CoA) Messages

The following tables list the RADIUS attributes and 3GPP VSAs supported by the MobileNext Broadband Gateway in RADIUS Change of Authorization (CoA) messages. CoA messages contain information for dynamically changing user session authorizations. They are typically used to change associated policies, filters, or QoS attributes.

- [RADIUS IETF Attributes Supported in CoA Messages on page 197](#)
- [3GPP VSAs Supported in CoA Messages on page 198](#)

### RADIUS IETF Attributes Supported in CoA Messages

[Table 30 on page 197](#) lists the RADIUS attributes supported by the broadband gateway in CoA messages.

Table 30: RADIUS IETF Attributes Supported in CoA Messages

Attribute Number	Attribute Name	Description	Content
1	User-Name	The username received in the Access-Request message, or a substitute username provided by the RADIUS server.  If a value for the User-Name attribute is received in the Access-Accept message, it takes precedence over any other value for the username.	String
4	NAS-IP-Address	IPv4 address of the broadband gateway for communication with the RADIUS server.	IPv4 address

Table 30: RADIUS IETF Attributes Supported in CoA Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
30	Called-Station-Id	Identifier for the target network (APN).	APN (UTF-8 encoded characters)
31	Calling-Station-ID	Identifier for the mobile station (MS), configurable on a per-APN basis.	MSISDN in international format, UTF-8 encoded decimal characters
32	NAS-Identifier	Identifier of the NAS originating the request.	String
44	Acct-Session-ID	User Session identifier, unique for every bearer under the session.  The broadband gateway performs the CoA action on the user session indicated by this attribute.	Broadband gateway Gn IP address (IPv4 or IPv6) and Charging-ID, concatenated in a UTF-8-encoded hexadecimal value

### 3GPP VSAs Supported in CoA Messages

Table 31 on page 198 lists the 3GPP vendor-specific attributes (VSAs) supported by the broadband gateway in CoA messages.

Table 31: 3GPP VSAs Supported in CoA Messages

Attribute Number	Attribute Name	Description	Content
26/10415/1 (3GPP type 1)	3GPP-IMSI	IMSI for this user.	UTF-8 encoded string
26/10415/2	3GPP-Charging-Id	Charging ID for this PDP context/EPS bearer.	Integer
26/10415/5	3GPP-GPRS-Negotiated-QoS-Profile	QoS profile to be applied by the broadband gateway for the PDP context/EPS bearer as the CoA action.	UTF-8 encoded string

- Related Documentation**
- [AAA Profiles on page 172](#)
  - [Configuring RADIUS Attribute Usage for an AAA Profile on page 207](#)
  - [Overview of AAA on the Broadband Gateway on page 167](#)

## CHAPTER 9

# Configuring AAA

- [Configuring AAA on the Broadband Gateway on page 199](#)
- [Configuring Interaction Between the Broadband Gateway and RADIUS Servers on page 200](#)
- [Configuring RADIUS-Initiated Dynamic Request Support on page 201](#)
- [Configuring Dead Server Detection on page 202](#)
- [Configuring Network Elements on page 203](#)
- [Configuring Network Element Groups on page 204](#)
- [Configuring an AAA Profile on page 204](#)
- [Configuring Authentication Settings in an AAA Profile on page 205](#)
- [Configuring Accounting Settings in an AAA Profile on page 205](#)
- [Configuring RADIUS Attribute Usage for an AAA Profile on page 207](#)
- [Specifying RADIUS Options in an AAA Profile on page 210](#)
- [Applying an AAA Profile to an APN on page 211](#)
- [Enabling Address Assignment by the RADIUS Server on page 211](#)
- [Configuring AAA-Assigned Addresses to Override Locally or DHCP-Assigned Addresses on page 212](#)
- [Configuring the Broadband Gateway to Wait for an Accounting Response on page 212](#)
- [Example: Configuring AAA on the Broadband Gateway on page 213](#)

## Configuring AAA on the Broadband Gateway

---

To configure authentication, authorization, and accounting (AAA) on the MobileNext Broadband Gateway:

1. Configure settings for the RADIUS servers.  
[See “Configuring Interaction Between the Broadband Gateway and RADIUS Servers” on page 200.](#)
2. Configure one or more network elements.  
[See “Configuring Network Elements” on page 203.](#)
3. (Optional) Configure a network element group to use with accounting.

See [“Configuring Network Element Groups” on page 204](#).

4. Configure an AAA profile.

See [“Configuring an AAA Profile” on page 204](#).

5. Configure AAA services for an APN.

See [“Applying an AAA Profile to an APN” on page 211](#).



**NOTE:** If you plan to make changes to AAA settings for an existing APN, or modify an AAA profile that has already been applied to an APN, then you must place the affected APNs into maintenance mode prior to making the changes.

---

**Related  
Documentation**

- [Overview of AAA on the Broadband Gateway on page 167](#)
- [Network Elements on page 171](#)
- [Network Element Groups on page 172](#)
- [AAA Profiles on page 172](#)
- [Mobility Maintenance Mode Overview on page 592](#)
- [Modifying an Access Point Name on page 596](#)

---

## Configuring Interaction Between the Broadband Gateway and RADIUS Servers

---

You specify the RADIUS servers that the MobileNext Broadband Gateway can use, and you configure how the broadband gateway interacts with the servers. After the RADIUS servers are configured, you can include them in network elements.

To specify a RADIUS server and how the broadband gateway interacts with the server:

1. Configure the name of the RADIUS server.

```
[edit]  
user@host# edit access radius servers radius1
```

2. Configure the IP address of the RADIUS server.

```
[edit access radius servers radius-server-name]  
user@host# set address 172.16.0.20
```

3. Configure an interface and IP address to specify the source address for RADIUS requests. The broadband gateway sends RADIUS requests to the RADIUS server using this source address.

```
[edit access radius servers radius-server-name]  
user@host# set source-interface lo0.0 ipv4-address 10.10.10.10
```

4. Configure the required secret (password) to use with the RADIUS server for authentication. Secrets enclosed in quotation marks can contain spaces.

```
[edit access radius servers radius-server-name]
```

```
user@host# set secret nt1UE1*7688+
```

5. (Optional) Configure the port number the broadband gateway uses for RADIUS authentication. The default port number is 1812.

```
[edit access radius servers radius-server-name]
user@host# set port 1812
```

6. (Optional) Configure the shared secret to be used for RADIUS accounting. If you do not specify a shared secret for accounting, the shared secret configured for RADIUS authentication is used for accounting.

```
[edit access radius servers radius-server-name]
user@host# set accounting-secret xp1UE1*4852+
```

7. (Optional) Configure the RADIUS server accounting port number. The default accounting port number is 1813.

```
[edit access radius servers radius-server-name]
user@host# set accounting-port 1813
```

8. (Optional) Configure the number of times that the broadband gateway attempts to contact the RADIUS server. You can specify from 1 to 10 retries. The default setting is 3 retry attempts.

```
[edit access radius servers radius-server-name]
user@host# set retry 4
```

9. (Optional) Configure the length of time that the broadband gateway waits to receive a response from a RADIUS server. By default, the broadband gateway waits 3 seconds. You can configure the timeout to be from 1 through 90 seconds.

```
[edit access radius servers radius-server-name]
user@host# set timeout 45
```

#### Related Documentation

- [Overview of AAA on the Broadband Gateway on page 167](#)
- [Example: Configuring AAA on the Broadband Gateway on page 213](#)

## Configuring RADIUS-Initiated Dynamic Request Support

When dynamic request support is enabled for a RADIUS server, the MobileNext Broadband Gateway uses the RADIUS server for both authentication and dynamic request operations, such as Change of Authorization (CoA) requests, Re-authorization requests, and Disconnect requests. The broadband gateway listens on UDP port 3799 for dynamic requests from the RADIUS server.

To configure dynamic request support for the RADIUS server:

1. Enable the broadband gateway to allow dynamic requests from the RADIUS server.

```
[edit access radius servers radius-server-name]
user@host# set allow-dynamic-requests
```



**NOTE:** If you allow dynamic requests from this RADIUS server, the combination of the address and source interface must be unique so that only one RADIUS server in the same VRF can be associated with any incoming dynamic requests.

2. (Optional) Configure the shared secret to be used for the dynamic requests. If you do not specify a shared secret for dynamic requests, the shared secret configured for RADIUS authentication is used.

```
[edit access radius servers radius-server-name]  
user@host# set dynamic-requests-secret 71UE1*4852+
```

**Related  
Documentation**

- [Overview of AAA on the Broadband Gateway on page 167](#)
- [Example: Configuring AAA on the Broadband Gateway on page 213](#)

---

## Configuring Dead Server Detection

The MobileNext Broadband Gateway detects when a RADIUS server is “dead” (that is, has stopped responding to requests), and starts directing requests to another server in the network element.

When a request sent by the broadband gateway to the RADIUS server times out, it retransmits the request to the server. If the request continues to time out, and does so for a given number of times over a given interval, the broadband gateway marks the server as “dead,” then starts sending requests to a different server in the network element. After a given number of seconds, the broadband gateway marks the dead server alive again, and can once again start sending requests to the server, according to the load-balancing algorithm and the server’s priority in the network element configuration.

To configure dead server detection, you specify the number of retransmissions and interval required to mark a server dead, and the amount of time after the server is marked dead that it is marked alive again.

To configure dead server detection for the RADIUS server.

1. Set the dead-criteria retries limit. This is the number of request retransmissions required to mark a server dead.

```
[edit access radius servers radius-server-name dead-criteria]  
user@host# set retries 100
```

2. Set the dead-criteria interval, in seconds. If the broadband gateway retransmits a request the number of times specified by the retries limit, over the number of seconds specified by the interval, the RADIUS server is marked dead.

```
[edit access radius servers radius-server-name dead-criteria]  
user@host# set interval 10
```

3. Set the dead server revert interval, in seconds. When a server is marked dead, the broadband gateway waits this amount of time, then marks the server alive again.



```
[edit access radius servers radius-server-name]
user@host# set revert-interval 10
```

**Related  
Documentation**

- [Overview of AAA on the Broadband Gateway on page 167](#)
- [Example: Configuring AAA on the Broadband Gateway on page 213](#)

## Configuring Network Elements

A network element is a load-balanced cluster of RADIUS servers. In an authentication, authorization, and accounting (AAA) profile, you select network elements to be used for authentication and accounting. When the AAA profile is applied to an access point name (APN), mobile subscribers attempting to get network access through the APN receive authentication or accounting services from one of the servers in the network element.

To configure a network element, you indicate the RADIUS servers that comprise it, optionally assign the servers a priority, and specify a load-balancing algorithm. You can also specify the maximum number of pending RADIUS requests that can be queued to the network element.

To configure a network element:

1. Specify the RADIUS servers that make up the network element.

```
[edit access radius network-elements network-element-name]
user@host# set server radius01
```

2. (Optional) Set the load-balancing algorithm for the network element. You can specify either direct or round-robin. The direct algorithm causes all requests to go to the first server configured in the network element; if that server cannot handle any additional requests (that is, the server is marked “dead”), they go to the next server in the list. The round-robin algorithm sends the first request to the first server in the list, the second request to the second server in the list, and so on; if a server is marked dead, it is removed from the round-robin selection rotation for the duration of the revert-interval.

```
[edit access radius network-elements network-element-name]
user@host# set algorithm round-robin
```

3. (Optional) Assign the RADIUS servers in the network element a priority of 1 or 2. The priority number is used for failover in case of server failure. The priority 2 servers are not used unless all the priority 1 servers fail. If all the priority 1 servers fail, then the broadband gateway starts using the priority 2 servers.

```
[edit access radius network-elements network-element-name server server-name]
user@host# set priority 1
```

4. (Optional) Specify the maximum number of requests that can be queued to the network element. When the pending request queue is full, any additional requests are dropped. If the number of pending requests reaches 80 percent of the maximum, an SNMP trap is generated. You can specify from 512 through 8192 for the pending request limit. The default is 8192.

```
[edit access radius network-elements network-element-name]
```

```
user@host# set maximum-pending-reqs-limit 4096
```

**Related  
Documentation**

- [Network Elements on page 171](#)
- [Network Element Groups on page 172](#)
- [Example: Configuring AAA on the Broadband Gateway on page 213](#)

---

## Configuring Network Element Groups

A network element group is a collection of network elements to which accounting request messages are sent.

To configure a network element group, you specify the network elements that comprise it, optionally indicate that a response is mandatory from a network element, and whether the MobileNext Broadband Gateway broadcasts accounting requests to all of the network elements in the group.

To configure a network element group:

1. Specify one or more network elements to make up the network element group.

```
[edit access radius network-element-group network-element-group-name]  
user@host# set network-element ne01
```

2. (Optional) Indicate that a response is mandatory from the network element when the broadband gateway sends it an accounting request.

```
[edit access radius network-element-group network-element-group-name]  
user@host# set network-element ne01 mandatory
```

3. (Optional) Specify that the broadband gateway broadcasts accounting requests to all network elements in the group.

```
[edit access radius network-element-group network-element-group-name]  
user@host# set broadcast
```

**Related  
Documentation**

- [Network Element Groups on page 172](#)
- [Network Elements on page 171](#)
- [Example: Configuring AAA on the Broadband Gateway on page 213](#)

---

## Configuring an AAA Profile

To configure an authentication, authorization, and accounting (AAA) profile:

1. Create the AAA profile.

```
[edit]  
user@host# edit unified-edge aaa mobile-profiles aaa-profile-name
```

2. Specify a network element to use for authentication.

See [“Configuring Authentication Settings in an AAA Profile” on page 205](#).

3. Configure accounting settings for the AAA profile.  
See [“Configuring Accounting Settings in an AAA Profile” on page 205](#).
4. (Optional) Specify which RADIUS attributes the MobileNext Broadband Gateway ignores or excludes from RADIUS messages.  
See [“Configuring RADIUS Attribute Usage for an AAA Profile” on page 207](#).
5. (Optional) Specify values for RADIUS attributes that the broadband gateway includes in RADIUS requests.  
See [“Specifying RADIUS Options in an AAA Profile” on page 210](#).

**Related Documentation**

- [Overview of AAA on the Broadband Gateway on page 167](#)
- [AAA Profiles on page 172](#)
- [Example: Configuring AAA on the Broadband Gateway on page 213](#)

---

## Configuring Authentication Settings in an AAA Profile

---

In an authentication, authorization, and accounting (AAA) profile, you specify which of the configured network elements you want to use for authentication. Users accessing the access point name (APN) to which the AAA profile is applied are authenticated using one of the RADIUS servers in the specified network element.

To configure authentication settings for an AAA profile:

- Enter the name of the configured network element to use for RADIUS authentication:  

```
[edit unified-edge aaa mobile-profiles aaaprofile radius authentication]  
user@host# set network-element ne01
```

**Related Documentation**

- [AAA Profiles on page 172](#)
- [Network Elements on page 171](#)
- [Example: Configuring AAA on the Broadband Gateway on page 213](#)

---

## Configuring Accounting Settings in an AAA Profile

---

To configure accounting settings for an authentication, authorization, and accounting (AAA) profile:

1. If you are using a network element for RADIUS accounting, enter the name of the configured network element to use.  

```
[edit unified-edge aaa mobile-profiles aaaprofile radius accounting]  
user@host# set network-element ne01
```
2. If you are using a network element group for RADIUS accounting, enter the name of the configured network element group to use.  

```
[edit unified-edge aaa mobile-profiles aaaprofile radius accounting]
```

```
user@host# set network-element-group ne-grp01
```



**NOTE:** In an AAA profile, you must specify either a network element or a network element group for accounting.

3. (Optional) Configure the MobileNext Broadband Gateway to send an Accounting-On message when a services PIC is restarted.

```
[edit unified-edge aaa mobile-profiles aaaprofile radius accounting]
user@host# set send-accounting-on
```

4. (Optional) Configure how often the broadband gateway sends accounting Interim-Update messages. You can specify from 10 through 1440 minutes. If you do not configure this option, the broadband gateway does not send accounting Interim-Update messages at regular intervals, but only when events listed in [Table 32 on page 206](#) occur.

```
[edit unified-edge aaa mobile-profiles aaaprofile radius accounting]
user@host# set trigger interim-interval 20
```

5. (Optional) Specify which events you want to exclude from triggering accounting Interim-Update messages. [Table 32 on page 206](#) lists the events you can specify.

```
[edit unified-edge aaa mobile-profiles aaaprofile radius accounting]
user@host# set trigger no-rat-change
```

**Table 32: Events You Can Exclude from Triggering Interim-Update Messages**

Event	CLI Entry to disable Interim-Updates for the event
The IPv4 address update for the mobile subscriber is deferred.	no-deferred-ipv4-address-update
The Mobile Station (MS) time zone changes.	no-ms-timezone-change
The Public Land Mobile Network (PLMN) to which the mobile subscriber is attached changes.	no-plmn-change
The QoS profile applied by the broadband gateway for the PDP context/EPS bearer changes.	no-qos-change
The Radio Access Technology (RAT) serving the mobile subscriber changes.	no-rat-change
The SGSN/S-GW serving the mobile subscriber changes.	no-sgw-change
The location information for the mobile subscriber changes.	no-user-location-information-change

- Related Documentation**
- [Overview of AAA on the Broadband Gateway on page 167](#)
  - [AAA Profiles on page 172](#)
  - [Network Elements on page 171](#)
  - [Network Element Groups on page 172](#)

- [Example: Configuring AAA on the Broadband Gateway on page 213](#)

## Configuring RADIUS Attribute Usage for an AAA Profile

In an authentication, authorization, and accounting (AAA) profile, you can specify which RADIUS attributes the MobileNext Broadband Gateway ignores in the RADIUS Access-Accept messages it receives, as well as which RADIUS attributes the broadband gateway excludes from specific types of RADIUS messages it sends to the RADIUS server. The broadband gateway supports a number of 3GPP vendor-specific attributes (VSAs). You can configure the AAA profile to exclude any or all of them from specified RADIUS message types.

To configure how RADIUS attributes are handled for an AAA profile:

1. Specify the RADIUS attributes you want the broadband gateway to ignore in Access-Accept messages. See [Table 33 on page 207](#) for the attributes you can configure.

```
[edit unified-edge aaa mobile-profiles aaaprofile radius attributes ignore]
user@host# set framed-ip-netmask
```

2. Specify which attributes the broadband gateway excludes from specific types of RADIUS messages it sends to the RADIUS server. See [Table 34 on page 208](#) for the RADIUS attributes and message type combinations you can configure. See [Table 35 on page 209](#) for the 3GPP VSAs and message type combinations you can configure.

The **all-3gpp** keyword causes the broadband gateway to exclude all of the 3GPP VSAs listed in [Table 35 on page 209](#) from the specified RADIUS message types.

```
[edit unified-edge aaa mobile-profiles aaaprofile radius attributes exclude]
user@host# set all-3gpp access-request
```

You use the **ignore** statement to configure the broadband gateway to ignore a particular attribute in RADIUS Access-Accept messages. By default, the broadband gateway processes the attributes received from the external RADIUS server. [Table 33 on page 207](#) lists the attributes supported in the **ignore** statement.

**Table 33: RADIUS Attributes the Broadband Gateway Can Ignore in Access-Accept Messages**

CLI Entry	Attribute Name	Attribute Number
framed-ip-netmask	Framed-Ip-Netmask	RADIUS attribute 9

You use the **exclude** statement to configure the broadband gateway to exclude the specified attributes from the specified type of RADIUS message. Not all attributes appear in all types of RADIUS messages—the CLI indicates the RADIUS message type. By default, the broadband gateway includes the specified attributes in RADIUS messages. [Table 34 on page 208](#) lists the RADIUS attributes and message types supported in the **exclude** statement.

**Table 34: RADIUS Attributes the Broadband Gateway Can Exclude from RADIUS Messages**

CLI Entry	Attribute Name	Attribute Number	Supported Message Type
accounting-authentic	Acct-Authentic	RADIUS attribute 45	Accounting-Start Accounting-Stop Accounting-Interim
accounting-delay-time	Acct-Delay-Time	RADIUS attribute 41	Accounting-Start Accounting-Stop Accounting-Interim
accounting-terminate-cause	Acct-Terminate-Cause	RADIUS attribute 49	Accounting-Stop
called-station-id	Called-Station-Id	RADIUS attribute 30	Access-Request Accounting-Start Accounting-Stop Accounting-Interim
calling-station-id	Calling-Station-Id	RADIUS attribute 31	Access-Request Accounting-Start Accounting-Stop Accounting-Interim
event-time-stamp	Event-Timestamp	RADIUS attribute 55	Accounting-Start Accounting-Stop Accounting-Interim
input-gigapackets	Acct-Input-Gigapackets	Juniper Networks VSA 26–42	Accounting-Stop Accounting-Interim
input-gigawords	Acct-Input-Gigawords	RADIUS attribute 52	Accounting-Stop Accounting-Interim
nas-identifier	NAS-Identifier	RADIUS attribute 32	Access-Request Accounting-Start Accounting-Stop

**Table 34: RADIUS Attributes the Broadband Gateway Can Exclude from RADIUS Messages** (*continued*)

CLI Entry	Attribute Name	Attribute Number	Supported Message Type
nas-ip-address	NAS-IP-Address	RADIUS attribute 4	Access-Request Accounting-Start Accounting-Stop Accounting-On Accounting-Interim
nas-port-type	NAS-Port-Type	RADIUS attribute 61	Access-Request
ouput-gigapackets	Acct-Output-Gigapackets	Juniper Networks VSA 26–43	Accounting-Stop Accounting-Interim
output-gigawords	Acct-Output-Gigawords	RADIUS attribute 53	Accounting-Stop Accounting-Interim

Table 35 on page 209 lists the 3GPP VSAs supported in the **exclude** statement. You can exclude individual 3GPP VSAs by entering the VSA's name in the CLI, or you can exclude all of the 3GPP VSAs by entering the **all-3gpp** keyword.

**Table 35: 3GPP VSAs That Can Be Excluded from RADIUS Messages**

CLI Entry	Attribute Name	Attribute Number	Supported Message Type
imeisv	3GPP-IMEISV	3GPP VSA 26–20	Access-Request Accounting-Start
imsi	3GPP-IMSI	3GPP VSA 26-1	Access-Request Accounting-Start Accounting-Stop Accounting-Interim
imsi-mcc-mnc	3GPP-IMSI-MCC-MNC	3GPP VSA 26-8	Access-Request Accounting-Start Accounting-Stop Accounting-Interim

**Table 35: 3GPP VSAs That Can Be Excluded from RADIUS Messages (*continued*)**

CLI Entry	Attribute Name	Attribute Number	Supported Message Type
sgsn-mcc-mnc	3GPP-SGSN-MCC-MNC	3GPP VSA 26-18	Access-Request
			Accounting-Start
			Accounting-Stop
			Accounting-Interim
user-location-info	3GPP-USER-LOCATION-INFO	3GPP VSA 26-22	Access-Request
			Accounting-Start
			Accounting-Stop
			Accounting-Interim

**Related Documentation**

- [Overview of AAA on the Broadband Gateway on page 167](#)
- [AAA Profiles on page 172](#)
- [Example: Configuring AAA on the Broadband Gateway on page 213](#)

## Specifying RADIUS Options in an AAA Profile

When configuring an authentication, authorization, and accounting (AAA) profile on the MobileNext Broadband Gateway, you can optionally specify values for a number of RADIUS attributes that the broadband gateway includes in the RADIUS messages it generates. You can specify a value for the NAS IP address attribute (RADIUS attribute 4), a prefix to be used with the NAS Identifier attribute (RADIUS attribute 32), and a value for the NAS Port Type attribute (RADIUS attribute 61).

To specify RADIUS options:

1. Specify a value for the `nas-ip-address` option. If this option is specified, the broadband gateway uses this IP address as the value for RADIUS attribute 4 (NAS-IP-Address) in RADIUS requests; otherwise, the broadband gateway uses the IP address set in the **source-interface** statement in the RADIUS server configuration.

```
[edit unified-edge aaa mobile-profiles aaaprofile radius options]
user@host# set nas-ip-address 172.16.0.20
```

2. Specify a value for the `nas-identifier-prefix` option. When this option is specified, the broadband gateway appends the ID of the services PIC to the `nas-identifier-prefix` value, and uses the combined prefix and services PIC ID as the value for RADIUS attribute 32 (NAS-Identifier) in RADIUS requests. If the services PICs are part of a redundancy group, the broadband gateway appends the aggregated multiservices interface (ams) ID to the prefix instead of the services PIC ID.

```
[edit unified-edge aaa mobile-profiles aaaprofile radius options]
```



```
user@host# set nas-identifier-prefix imagio
```

3. Specify a value for the nas-port-type option. In an AAA profile, you can specify a NAS port type of virtual or wireless. The broadband gateway uses this as the value for RADIUS attribute 61 (NAS-Port-Type) in RADIUS requests. The default is virtual.

```
[edit unified-edge aaa mobile-profiles aaaprofile radius options]  
user@host# set nas-port-type wireless
```

**Related  
Documentation**

- [AAA Profiles on page 172](#)
- [Example: Configuring AAA on the Broadband Gateway on page 213](#)

---

## Applying an AAA Profile to an APN

To apply an authentication, authorization, and accounting (AAA) profile to an access point name (APN):

1. Indicate that you want to configure services for a particular APN.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services]  
user@host# edit apn apn-name
```

2. Specify the name of the AAA profile you want to apply to this APN.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-name]  
user@host# set aaa-profile aaa-profile-name
```

**Related  
Documentation**

- [Configuring APNs on the MobileNext Broadband Gateway Overview on page 113](#)
- [AAA Profiles on page 172](#)
- [Example: Configuring AAA on the Broadband Gateway on page 213](#)

---

## Enabling Address Assignment by the RADIUS Server

You can optionally configure the MobileNext Broadband Gateway to allow the RADIUS server to assign addresses to mobile subscribers. If this option is configured, the broadband gateway uses the address received in the Framed-IP-Address attribute (RADIUS attribute 8) of the Access-Accept message as the IP address for the subscriber.

If this option is not configured, the IP addresses are assigned locally by the broadband gateway using the address pool or group configured on the access point name (APN).

- To enable address assignment by the RADIUS server:

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-name]  
user@host# set address-assignment aaa
```

**Related  
Documentation**

- [Configuring Address Assignment on a Broadband Gateway APN on page 122](#)
- [Example: Configuring AAA on the Broadband Gateway on page 213](#)

## Configuring AAA-Assigned Addresses to Override Locally or DHCP-Assigned Addresses

If the configured address-assignment method for the access point name (APN) is set to **local** or **dhcp-proxy-client**, then the MobileNext Broadband Gateway assigns addresses to mobile subscribers using one of these methods. You can optionally configure the broadband gateway so that if an address is also assigned to the mobile subscriber by a RADIUS server, then the RADIUS-assigned address is used in place of the locally assigned or DHCP-assigned address.

- To configure AAA-assigned addresses to override locally assigned addresses:

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-name
address-assignment]
user@host# set address-assignment local aaa-override
```

- To configure AAA-assigned addresses to override DHCP-assigned addresses:

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-name
address-assignment]
user@host# set address-assignment dhcp-proxy-client aaa-override
```

### Related Documentation

- [Configuring Address Assignment on a Broadband Gateway APN on page 122](#)
- [Example: Configuring AAA on the Broadband Gateway on page 213](#)

## Configuring the Broadband Gateway to Wait for an Accounting Response

When accounting is configured for an access point name (APN), the MobileNext Broadband Gateway generates an Accounting Start message when it receives a Create Session Request or Create PDP Context Request message from the user equipment. By default, the broadband gateway does not wait for the accounting response from the RADIUS server before sending the Create Session Response or Create PDP Context Response message.

You can optionally configure the broadband gateway to send the Create Session Response or Create PDP Context Response message only after it receives the Accounting Start Response message from the RADIUS server.

- To configure the broadband gateway to wait for an accounting response before creating a session for the user equipment:

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-name]
user@host# set wait-accounting
```

### Related Documentation

- [Overview of AAA on the Broadband Gateway on page 167](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 117](#)

## Example: Configuring AAA on the Broadband Gateway

---

- [Requirements on page 213](#)
- [Overview on page 213](#)
- [Configuration on page 215](#)
- [Verification on page 223](#)

### Requirements

This example uses the following hardware and software components:

- Junos OS Release 11.2W
- Juniper Networks MobileNext Broadband Gateway, including the following components:
  - MX240 3D Universal Edge Router, MX480 3D Universal Edge Router, or MX960 3D Universal Edge Router
  - Mobile Multiservices DPC (MS-DPC)
  - Mobile 10-Gigabit Ethernet MPC with SFP+ or Mobile 60-Gigabit Ethernet Enhanced Queuing MPC line card

### Overview

This example documents an authentication, authorization, and accounting (AAA) configuration where the broadband gateway interacts with a collection of RADIUS servers to provide AAA services to mobile subscribers accessing an access point name (APN). The RADIUS servers are configured into network elements, and some of the network elements are placed into a network element group. One of the network elements provides authentication services, and the network element group receives the accounting messages.

One of the RADIUS servers is configured to provide support for dynamic requests, such as Change of Authorization (CoA) requests and Disconnect requests. Note that this dynamic request server is not part of a network element.

The APN is configured to use the RADIUS server for IP address assignment. When a mobile subscriber is authenticated, the Access-Accept message specifies the IP address to be assigned to the subscriber. If a mobile subscriber cannot be authenticated based on the contents of the Create PDP Context Request or Create Session Request message, then the mobile subscriber is authenticated with the username of "aaa" and the password "Password123."

The AAA configuration example consists of the following parts:

1. Configuring the RADIUS servers.

This part of the configuration establishes settings for the dynamic request server, *radiusDR*, and eight other RADIUS servers, *radius1* through *radius8*. The configurations for the RADIUS servers are basically identical, with some minor differences. Server *radiusDR* has dynamic requests enabled, which means that the broadband gateway acts upon CoA requests and Disconnect requests originating from the *radiusDR* server.

Also note that dead server detection is configured for the RADIUS servers: the **dead-criteria retries 10 interval 10** and **revert-interval 100** statements mean that if the broadband gateway has to retransmit a request to the server 10 times over a 10-second interval, the server is marked “dead”, and the broadband gateway starts sending requests to a different server. After the revert-interval of 100 seconds, the server is marked “alive,” and the broadband gateway can direct requests to it again.

2. Configuring the loopback interface.

This part of the configuration set addresses on the lo0 interface for the dynamic request server and for the other RADIUS servers.

3. Configuring the network elements.

This part of the configuration creates three network elements: *ne1*, *ne2*, and *ne3*, which are made up of the RADIUS servers configured in part 1. In network element *ne1*, the *radius1* and *radius2* servers are configured as priority 1, and *radius3* is priority 2. The load-balancing algorithm is configured as Direct. When the broadband gateway sends requests to *ne1*, they go only to the *radius1* server, up to the point where *radius1* is marked dead. At that point, they go to *radius2*. Once the revert-interval configured for *radius1* (100 seconds) expires, the broadband gateway can start directing requests to *radius1* again. Only if both priority 1 servers are marked dead does the broadband gateway start sending requests to the priority 2 server, *radius3*.

Network elements *ne2* and *ne3* both use the round-robin load-balancing algorithm. When sending requests to *ne2*, the broadband gateway sends the first request to *radius4*, the second request to *radius5*, the third to *radius4*, and so on. For *ne3*, since *radius6* and *radius7* are priority 1 servers, the broadband gateway alternates requests between the two servers. If both of the servers are marked dead, then the broadband gateway sends requests to the priority 2 server, *radius8*.

4. Configuring the network element group.

This part of the configuration creates a network element group, *ne-grp1*, consisting of network elements *ne2* and *ne3*, which were configured in part 2. The broadband gateway sends accounting messages to the network elements in the group.

In the example, the **broadcast** parameter is specified, which causes the broadband gateway to send the accounting messages to all of the network elements in the group. The **mandatory** option is configured for network element *ne2*, which means that a response is required from a server in *ne2* before services can be provided to the mobile subscriber. If you configure the **broadcast** parameter for a network element group, you must specify the **mandatory** parameter for at least one of the network elements.

5. Configuring the AAA profile.

This part of the configuration sets up an AAA profile, *aaa-prof*. The AAA profile specifies that network element *ne1* is used for authentication, and network element group *ne-grp01* is used for accounting.

For accounting, Interim-Update messages are sent every 10 minutes, and when any of the trigger events occur. The one exception is if the QoS profile applied by the broadband gateway for the PDP context/EPS bearer changes; that is, the broadband gateway receives an accounting message with a 3GPP-GPRS-Negotiated-QoS-Profile attribute (3GPP VSA 26-5) that has a value different from the one previously received. In this case, it does not trigger the broadband gateway to send an Interim-Update message.

In the RADIUS messages it generates, the broadband gateway sets values for the following RADIUS attributes:

- For the NAS-Identifier attribute (RADIUS attribute 32), the value is the string *imago*, prefixed to the ID of the services PIC handling NAS functions for the mobile subscriber.
- For the NAS-Port-Type attribute (RADIUS attribute 61), the value is set to *wireless*.

The broadband gateway excludes certain RADIUS attributes from specific types of RADIUS messages it generates:

- The Called-Station-Id attribute (RADIUS attribute 30) is excluded from Access-Request messages.
- The Event-Timestamp attribute (RADIUS attribute 55) is excluded from Accounting Start messages.

The broadband gateway ignores the Framed-Ip-Netmask attribute (RADIUS attribute 9) in Access-Accept messages it receives from the RADIUS server.

#### 6. Applying AAA services to an APN.

This part of the configuration applies AAA services to an APN, *internet123*. The AAA services are configured for the APN by specifying the AAA profile to use—in this case, *aaa-prof*—configured in the previous part. When mobile subscribers attempt to gain access to this APN, they receive AAA services as indicated by the settings in the *aaa-prof* profile.

In addition, the APN is configured to use AAA as the address assignment method. This means that the broadband gateway assigns an IP address to a mobile subscriber using information returned from the RADIUS server in the Access-Accept message.

If the broadband gateway cannot determine the subscriber's username and password from the Create PDP Context Request or Create Session Request message or if the **override-pco** statement is configured under **user-options**, then the username and password configured under **user-options**, in the APN configuration, are used to authenticate the subscriber.

## Configuration

- [Configuring the RADIUS Servers on page 216](#)
- [Configuring the Loopback Interface on page 219](#)

- [Configuring the Network Elements on page 219](#)
- [Configuring the Network Element Group on page 220](#)
- [Configuring the AAA Profile on page 221](#)
- [Applying AAA Services to an APN on page 222](#)

---

### Configuring the RADIUS Servers

---

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set access radius servers radiusDR address 50.50.50.110
set access radius servers radiusDR secret "$9$BWYErVx7VY2axNs4oJkq"
set access radius servers radiusDR allow-dynamic-requests
set access radius servers radiusDR dynamic-request-secret "$9$rXYKWxbs4Di.Ndi"
set access radius servers radiusDR source-interface lo0.0 ipv4-address 200.6.80.1

set access radius servers radius1 address 200.6.101.2
set access radius servers radius1 secret "$9$BWYErVx7VY2axNs4oJkq"
set access radius servers radius1 accounting-secret "$9$rpEvX-Y2aUDkYgGiHqzF"
set access radius servers radius1 dead-criteria retries 10 interval 10
set access radius servers radius1 revert-interval 100
set access radius servers radius1 source-interface lo0.0 ipv4-address 200.6.88.1

set access radius servers radius2 address 200.6.102.2
set access radius servers radius2 secret "$9$BWYErVx7VY2axNs4oJkq"
set access radius servers radius2 accounting-secret "$9$rpEvX-Y2aUDkYgGiHqzF"
set access radius servers radius2 dead-criteria retries 10 interval 10
set access radius servers radius2 revert-interval 100
set access radius servers radius2 source-interface lo0.0 ipv4-address 200.6.88.1

set access radius servers radius3 address 200.6.103.2
set access radius servers radius3 secret "$9$BWYErVx7VY2axNs4oJkq"
set access radius servers radius3 accounting-secret "$9$rpEvX-Y2aUDkYgGiHqzF"
set access radius servers radius3 dead-criteria retries 10 interval 10
set access radius servers radius3 revert-interval 100
set access radius servers radius3 source-interface lo0.0 ipv4-address 200.6.88.1

set access radius servers radius4 address 200.6.104.2
set access radius servers radius4 secret "$9$BWYErVx7VY2axNs4oJkq"
set access radius servers radius4 accounting-secret "$9$rpEvX-Y2aUDkYgGiHqzF"
set access radius servers radius4 dead-criteria retries 10 interval 10
set access radius servers radius4 revert-interval 100
set access radius servers radius4 source-interface lo0.0 ipv4-address 200.6.88.1

set access radius servers radius5 address 200.6.105.2
set access radius servers radius5 secret "$9$BWYErVx7VY2axNs4oJkq"
set access radius servers radius5 accounting-secret "$9$rpEvX-Y2aUDkYgGiHqzF"
set access radius servers radius5 dead-criteria retries 10 interval 10
set access radius servers radius5 revert-interval 100
set access radius servers radius5 source-interface lo0.0 ipv4-address 200.6.88.1
```

```

set access radius servers radius6 address 200.6.106.2
set access radius servers radius6 secret "$9$BWYErVx7VY2axNs4oJkq"
set access radius servers radius6 accounting-secret "$9$rpEvX-Y2aUDkYgGiHqzF"
set access radius servers radius6 dead-criteria retries 10 interval 10
set access radius servers radius6 revert-interval 100
set access radius servers radius6 source-interface lo0.0 ipv4-address 200.6.88.1

```

```

set access radius servers radius7 address 200.6.107.2
set access radius servers radius7 secret "$9$BWYErVx7VY2axNs4oJkq"
set access radius servers radius7 accounting-secret "$9$rpEvX-Y2aUDkYgGiHqzF"
set access radius servers radius7 dead-criteria retries 10 interval 10
set access radius servers radius7 revert-interval 100
set access radius servers radius7 source-interface lo0.0 ipv4-address 200.6.88.1

```

```

set access radius servers radius8 address 200.6.108.2
set access radius servers radius8 secret "$9$BWYErVx7VY2axNs4oJkq"
set access radius servers radius8 accounting-secret "$9$rpEvX-Y2aUDkYgGiHqzF"
set access radius servers radius8 dead-criteria retries 10 interval 10
set access radius servers radius8 revert-interval 100
set access radius servers radius8 source-interface lo0.0 ipv4-address 200.6.88.1

```

### Step-by-Step Procedure

To configure the RADIUS servers:

1. Configure the settings for the dynamic request server, radiusDR. Enable dynamic request support, and specify a shared secret for dynamic request messages.

```

[edit]
user@pe1# set access radius servers radiusDR address 50.50.50.110
user@pe1# set access radius servers radiusDR secret "$9$BWYErVx7VY2axNs4oJkq"
user@pe1# set access radius servers radiusDR allow-dynamic-requests
user@pe1# set access radius servers radiusDR dynamic-request-secret
"$9$rXYKWxbs4Di.Ndi"
user@pe1# set access radius servers radiusDR source-interface lo0.0 ipv4-address
200.6.80.1

```

2. Configure the settings for the radius1 server.

```

[edit]
user@pe1# set access radius servers radius1 address 200.6.101.2
user@pe1# set access radius servers radius1 secret "$9$BWYErVx7VY2axNs4oJkq"
user@pe1# set access radius servers radius1 accounting-secret
"$9$rpEvX-Y2aUDkYgGiHqzF"
user@pe1# set access radius servers radius1 dead-criteria retries 10 interval 10
user@pe1# set access radius servers radius1 revert-interval 100
user@pe1# set access radius servers radius1 source-interface lo0.0 ipv4-address
200.6.88.1

```



**NOTE:** Apart from the server name and address, the configuration of servers radius2 through radius8 is identical.

3. Configure the settings for the radius2 server.

```

[edit]

```

```
user@pe1# set access radius servers radius2 address 200.6.102.2
user@pe1# set access radius servers radius2 secret "$9$BWYErVx7VY2axNs4oJkq"
user@pe1# set access radius servers radius2 accounting-secret
"$9$rpEvX-Y2aUDkYgGiHqzF"
user@pe1# set access radius servers radius2 dead-criteria retries 10 interval 10
user@pe1# set access radius servers radius2 revert-interval 100
user@pe1# set access radius servers radius2 source-interface lo0.0 ipv4-address
200.6.88.1
```

4. Configure the settings for the radius3 server.

```
[edit]
user@pe1# set access radius servers radius3 address 200.6.103.2
user@pe1# set access radius servers radius3 secret "$9$BWYErVx7VY2axNs4oJkq"
user@pe1# set access radius servers radius3 accounting-secret
"$9$rpEvX-Y2aUDkYgGiHqzF"
user@pe1# set access radius servers radius3 dead-criteria retries 10 interval 10
user@pe1# set access radius servers radius3 revert-interval 100
user@pe1# set access radius servers radius3 source-interface lo0.0 ipv4-address
200.6.88.1
```

5. Configure the settings for the radius4 server.

```
[edit]
user@pe1# set access radius servers radius4 address 200.6.104.2
user@pe1# set access radius servers radius4 secret "$9$BWYErVx7VY2axNs4oJkq"
user@pe1# set access radius servers radius4 accounting-secret
"$9$rpEvX-Y2aUDkYgGiHqzF"
user@pe1# set access radius servers radius4 dead-criteria retries 10 interval 10
user@pe1# set access radius servers radius4 revert-interval 100
user@pe1# set access radius servers radius4 source-interface lo0.0 ipv4-address
200.6.88.1
```

6. Configure the settings for the radius5 server.

```
[edit]
user@pe1# set access radius servers radius5 address 200.6.105.2
user@pe1# set access radius servers radius5 secret "$9$BWYErVx7VY2axNs4oJkq"
user@pe1# set access radius servers radius5 accounting-secret
"$9$rpEvX-Y2aUDkYgGiHqzF"
user@pe1# set access radius servers radius5 dead-criteria retries 10 interval 10
user@pe1# set access radius servers radius5 revert-interval 100
user@pe1# set access radius servers radius5 source-interface lo0.0 ipv4-address
200.6.88.1
```

7. Configure the settings for the radius6 server.

```
[edit]
user@pe1# set access radius servers radius6 address 200.6.106.2
user@pe1# set access radius servers radius6 secret "$9$BWYErVx7VY2axNs4oJkq"
user@pe1# set access radius servers radius6 accounting-secret
"$9$rpEvX-Y2aUDkYgGiHqzF"
user@pe1# set access radius servers radius6 dead-criteria retries 10 interval 10
user@pe1# set access radius servers radius6 revert-interval 100
user@pe1# set access radius servers radius6 source-interface lo0.0 ipv4-address
200.6.88.1
```

8. Configure the settings for the radius7 server.



```
[edit]
user@pe1# set access radius servers radius7 address 200.6.107.2
user@pe1# set access radius servers radius7 secret "$9$BWYervx7VY2axNs4oJkq"
user@pe1# set access radius servers radius7 accounting-secret
"$9$rpEvX-Y2aUDkYgGiHqzF"
user@pe1# set access radius servers radius7 dead-criteria retries 10 interval 10
user@pe1# set access radius servers radius7 revert-interval 100
user@pe1# set access radius servers radius7 source-interface lo0.0 ipv4-address
200.6.88.1
```

9. Configure the settings for the radius8 server.

```
[edit]
user@pe1# set access radius servers radius8 address 200.6.108.2
user@pe1# set access radius servers radius8 secret "$9$BWYervx7VY2axNs4oJkq"
user@pe1# set access radius servers radius8 accounting-secret
"$9$rpEvX-Y2aUDkYgGiHqzF"
user@pe1# set access radius servers radius8 dead-criteria retries 10 interval 10
user@pe1# set access radius servers radius8 revert-interval 100
user@pe1# set access radius servers radius8 source-interface lo0.0 ipv4-address
200.6.88.1
```

### Configuring the Loopback Interface

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set interfaces lo0 unit 0 family inet address 200.6.80.1/32
set interfaces lo0 unit 0 family inet address 200.6.88.1/32
```

**Step-by-Step Procedure** 1. Configure a loopback address for the dynamic request server. The dynamic request server uses this as the destination address for CoA requests and Disconnect requests.

```
[edit]
user@pe1# set interfaces lo0 unit 0 family inet address 200.6.80.1/32
```

2. Configure a loopback address for the other RADIUS servers.

```
[edit]
user@pe1# set interfaces lo0 unit 0 family inet address 200.6.88.1/32
```

### Configuring the Network Elements

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set access radius network-elements ne1 server radius1 priority 1
set access radius network-elements ne1 server radius2 priority 1
set access radius network-elements ne1 server radius3 priority 2
set access radius network-elements ne1 algorithm direct
set access radius network-elements ne1 maximum-pending-reqs-limit 2048

set access radius network-elements ne2 server radius4 priority 1
set access radius network-elements ne2 server radius5 priority 1
```

```
set access radius network-elements ne2 algorithm round-robin
```

```
set access radius network-elements ne3 server radius6 priority 1
set access radius network-elements ne3 server radius7 priority 1
set access radius network-elements ne3 server radius8 priority 2
set access radius network-elements ne3 algorithm round-robin
```

**Step-by-Step  
Procedure**

To configure the network elements:

1. Configure the settings for network element ne1. Add RADIUS servers radius1, radius2, and radius3, set the load-balancing algorithm to direct, and set the maximum pending requests limit to 2048.

```
[edit]
user@pe1# set access radius network-elements ne1 server radius1 priority 1
user@pe1# set access radius network-elements ne1 server radius2 priority 1
user@pe1# set access radius network-elements ne1 server radius3 priority 2
user@pe1# set access radius network-elements ne1 algorithm direct
user@pe1# set access radius network-elements ne1 maximum-pending-reqs-limit
2048
```

2. Configure the settings for network element ne2. Add RADIUS servers radius4 and radius5, and set the load-balancing algorithm to round-robin.

```
[edit]
user@pe1# set access radius network-elements ne2 server radius4 priority 1
user@pe1# set access radius network-elements ne2 server radius5 priority 1
user@pe1# set access radius network-elements ne2 algorithm round-robin
```

3. Configure the settings for network element ne3. Add RADIUS servers radius6, radius7, and radius8, and set the load-balancing algorithm to round-robin.

```
[edit]
user@pe1# set access radius network-elements ne3 server radius6 priority 1
user@pe1# set access radius network-elements ne3 server radius7 priority 1
user@pe1# set access radius network-elements ne3 server radius8 priority 2
user@pe1# set access radius network-elements ne3 algorithm round-robin
```

---

### Configuring the Network Element Group

**CLI Quick  
Configuration**

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set access radius network-element-group ne-grp1 network-element ne2 mandatory
set access radius network-element-group ne-grp1 network-element ne3
set access radius network-element-group ne-grp1 broadcast
```

**Step-by-Step  
Procedure**

To configure the network element group:

1. Add network elements ne2 and ne3 to network element group ne-grp1, and indicate that a response from ne2 is mandatory in order to provide services to the mobile subscriber.

```
[edit]
```

```
user@pe1# set access radius network-element-group ne-grp1 network-element ne2
mandatory
```

```
user@pe1# set access radius network-element-group ne-grp1 network-element ne3
```

2. Configure accounting messages to be broadcast to all of the network elements in the group.

```
[edit]
```

```
user@pe1# set access radius network-element-group ne-grp1 broadcast
```

### Configuring the AAA Profile

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
```

```
set unified-edge aaa mobile-profiles aaa-prof radius authentication network-element ne1
```

```
set unified-edge aaa mobile-profiles aaa-prof radius accounting network-element-group ne-grp1
```

```
set unified-edge aaa mobile-profiles aaa-prof radius accounting trigger interim-interval 10
```

```
set unified-edge aaa mobile-profiles aaa-prof radius accounting trigger no-qos-change
```

```
set unified-edge aaa mobile-profiles aaa-prof radius options nas-identifier-prefix imago
```

```
set unified-edge aaa mobile-profiles aaa-prof radius options nas-port-type wireless
```

```
set unified-edge aaa mobile-profiles aaa-prof radius options nas-ip-address 200.6.80.1
```

```
set unified-edge aaa mobile-profiles aaa-prof radius attributes exclude called-station-id access-request
```

```
set unified-edge aaa mobile-profiles aaa-prof radius attributes exclude event-time-stamp accounting-start
```

```
set unified-edge aaa mobile-profiles aaa-prof radius attributes ignore framed-ip-netmask
```

#### Step-by-Step Procedure

To configure the AAA profile:

1. Indicate that network element ne1 is to be used for authentication.

```
[edit]
```

```
user@pe1# set unified-edge aaa mobile-profiles aaa-prof radius authentication network-element ne1
```

2. Indicate that network element group ne-grp1 is to be used for accounting.

```
[edit]
```

```
user@pe1# set unified-edge aaa mobile-profiles aaa-prof radius accounting network-element-group ne-grp1
```

3. Configure the broadband gateway to send accounting Interim-Update messages every 10 minutes.

```
[edit]
```

```
user@pe1# set unified-edge aaa mobile-profiles aaa-prof radius accounting trigger interim-interval 10
```

4. Configure the broadband gateway so that it does not trigger an accounting Interim-Update message if the QoS profile applied to the PDP context/EPS bearer changes.

```
[edit]
```

```
user@pe1# set unified-edge aaa mobile-profiles aaa-prof radius accounting trigger  
no-qos-change
```

5. Configure the broadband gateway to set the NAS-Identifier attribute in RADIUS messages to the string *imago*, prefixed to the ID of the services PIC handling NAS functions for the mobile subscriber.

```
[edit]  
user@pe1# set unified-edge aaa mobile-profiles aaa-prof radius options  
nas-identifier-prefix imago
```

6. Configure the broadband gateway to set the NAS-Port-Type attribute in RADIUS messages to *wireless*.

```
[edit]  
user@pe1# set unified-edge aaa mobile-profiles aaa-prof radius options  
nas-port-type wireless
```

7. Configure the broadband gateway to use 200.6.80.1 as the value for the NAS-IP-Address attribute in RADIUS requests. (This causes the CoA requests and Disconnect requests sent from the dynamic request server to have a source address of 50.50.50.110 and a destination address of 200.6.80.1.)

```
[edit]  
user@pe1# set unified-edge aaa mobile-profiles aaa-prof radius options  
nas-ip-address 200.6.80.1
```

8. Configure the broadband gateway to exclude the Called-Station-Id attribute from RADIUS Access-Request messages.

```
[edit]  
user@pe1# set unified-edge aaa mobile-profiles aaa-prof radius attributes exclude  
called-station-id access-request
```

9. Configure the broadband gateway to exclude the Event-Timestamp attribute from RADIUS Accounting Start messages.

```
[edit]  
user@pe1# set unified-edge aaa mobile-profiles aaa-prof radius attributes exclude  
event-time-stamp accounting-start
```

10. Configure the broadband gateway to ignore the Framed-Ip-Netmask attribute in Access-Accept messages it receives from the RADIUS server.

```
[edit]  
user@pe1# set unified-edge aaa mobile-profiles aaa-prof radius attributes ignore  
framed-ip-netmask
```

---

### Applying AAA Services to an APN

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]  
set unified-edge gateways ggsn-pgw MBG1 apn-services apns internet123 apn-data-type  
ipv4  
set unified-edge gateways ggsn-pgw MBG1 apn-services apns internet123 mobile-interface  
mif.0
```

```

set unified-edge gateways ggsn-pgw MBG1 apn-services apns internet123 aaa-profile
aaa-prof
set unified-edge gateways ggsn-pgw MBG1 apn-services apns internet123
address-assignment aaa
set unified-edge gateways ggsn-pgw MBG1 apn-services apns internet123 user-options
user-name aaa
set unified-edge gateways ggsn-pgw MBG1 apn-services apns internet123 user-options
password "Password123"

```

### Step-by-Step Procedure

To configure AAA services for the APN:

1. If not set already, set the data type and mobile interface for APN internet123.
 

```

[edit]
user@pe1# set unified-edge gateways ggsn-pgw MBG1 apn-services apns internet123
apn-data-type ipv4
user@pe1# set unified-edge gateways ggsn-pgw MBG1 apn-services apns internet123
mobile-interface mif.0

```
2. Configure the APN to use the settings in the *aaa-prof* AAA profile.
 

```

[edit]
user@pe1# set unified-edge gateways ggsn-pgw MBG1 apn-services apns internet123
aaa-profile aaa-prof

```
3. Configure the broadband gateway to use the AAA server for IP address assignment. IP addresses are assigned to mobile subscribers using information returned in RADIUS Access-Accept messages.
 

```

[edit]
user@pe1# set unified-edge gateways ggsn-pgw MBG1 apn-services apns internet123
address-assignment aaa

```
4. Configure the broadband gateway to authenticate a mobile subscriber using the username "aaa" and the password "Password123" if username and password information cannot be determined from the Protocol Configuration Options (PCO) received in the Create PDP Context Request or Create Session Request message.
 

```

[edit]
user@pe1# set unified-edge gateways ggsn-pgw MBG1 apn-services apns internet123
user-options user-name aaa
user@pe1# set unified-edge gateways ggsn-pgw MBG1 apn-services apns internet123
user-options password "Password123"

```

## Verification

### Verifying Authentication

**Purpose** Verify that authentication functions are working on the broadband gateway and for the individual RADIUS servers.

**Action** To show authentication statistics for the broadband gateway:

```
user@host> show unified-edge ggsn-pgw aaa statistics authentication
Authentication module statistics
Requests: 3
Accepts: 3
Rejects: 0
Challenges: 0
Requests timed out: 0
Transmit errors: 0
Response errors: 0
Pending requests: 0
```

To show authentication statistics for an individual RADIUS server:

```
user@host> show unified-edge ggsn-pgw aaa radius statistics authentication detail name radius1
RADIUS server: radius1 (FPC/PIC: 1/0)
Address: 200.6.101.2 Port: 1812
Routing-instance: default
State: Active Duration: 00:28:01
Prev duration: 00:00:00 Flaps: 0
Access requests: 0
Access req retransmissions: 0
Access accepts: 0
Access rejects: 0
Access challenges: 0
Malformed responses: 0
Bad authenticators: 0
Pending requests: 0
Timeouts: 0
Unknown types: 0
Packets dropped: 0
Round trip time (ms): 0 (Min: 0 Max: 0 Avg: 0)
Time since counters were last cleared: 00:00:00
```

---

### Verifying Accounting

**Purpose** Verify that accounting functions are working on the broadband gateway and for the individual RADIUS servers.

**Action** To show accounting statistics for the broadband gateway:

```
user@host> show unified-edge ggsn-pgw aaa statistics accounting
Accounting module statistics
  Requests: 12
  Responses success: 12
  Requests timed out: 0
  Transmit errors: 0
  Response errors: 0
  Pending requests: 0
```

To show accounting statistics for an individual RADIUS server:

```
user@host> show unified-edge ggsn-pgw aaa radius statistics accounting detail name radius1
RADIUS server: radius1 (FPC/PIC: 1/0)
  Address: 200.6.101.2 Port: 1813
  Routing-instance: default
  State: Active Duration: 00:28:21
  Prev duration: 00:00:00 Flaps: 0
  Accounting requests: 0
    Start: 0 Stop: 0 Interim: 0 On: 0 Off: 0
  Accounting req retransmissions: 0
  Accounting responses: 0
  Malformed responses: 0
  Bad authenticators: 0
  Pending requests: 0
  Timeouts: 0
  Unknown types: 0
  Packets dropped: 0
  Round trip time (ms): 0 (Min: 0 Max: 0 Avg: 0)
  Time since counters were last cleared: 00:00:00
```

---

### Verifying Dynamic Requests

**Purpose** Verify that dynamic request functions are working on the broadband gateway and for the dynamic request server.

**Action** To show dynamic request statistics for the broadband gateway:

```
user@host> show unified-edge ggsn-pgw aaa statistics dynamic-requests
Dynamic Requests module statistics
Requests received: 8
CoA Requests received: 8
Dm Requests received: 0
CoA Acks sent: 7
CoA Nacks sent: 1
Dm Acks sent: 0
Dm Nacks sent: 0
Dropped: 0
```

To show dynamic request statistics for the dynamic request server radiusDR:

```
user@host> show unified-edge ggsn-pgw aaa radius statistics dynamic-requests detail name
radiusDR
RADIUS client: radiusDR (FPC/PIC: 3/0)
Address: 50.50.50.110
CoA Requests received: 0
Dm Requests received: 0
CoA Acks sent: 0
CoA Nacks sent: 0
Dm Acks sent: 0
Dm Nacks sent: 0
Dropped: 0
Duplicates: 0
Dispatched: 0
Timeouts: 0
Sent to SMD: 0
Invalid RADIUS codes: 0
Errors during processing: 0
Invalid RADIUS authenticators: 0
Invalid or missing Charging Ids: 0
RCM errors: 0
Time since counters were last cleared: 00:00:00
```

---

### Verifying Network Element Status

**Purpose** Verify that the RADIUS servers in the network elements are active.

**Action**

```
user@host> show unified-edge ggsn-pgw aaa network-element status name ne1
Network-element: ne1
Server: radius1, Priority: 1, State: Active
Server: radius2, Priority: 1, State: Active
Server: radius3, Priority: 2, State: Active
```

---

### Verifying Address Assignment

**Purpose** Verify that address assignment by the AAA server is working properly.



**Action**    `user@host> show unified-edge ggsn-pgw address-assignment statistics`  
Address assignment statistics  
Total address allocations: 0  
Total allocation failures: 0  
Total address releases: 0

- Related Documentation**
- [Overview of AAA on the Broadband Gateway on page 167](#)
  - [Configuring AAA on the Broadband Gateway on page 199](#)
  - [Configuring APNs on the MobileNext Broadband Gateway Overview on page 113](#)
  - [Configuring User Options on a Broadband Gateway APN on page 141](#)
  - [Configuring Address Assignment on a Broadband Gateway APN on page 122](#)



# Configuring Address Assignment

- Overview of Mobile Pools and Mobile Pool Groups for the Broadband Gateway on page 229
- Configuring Mobile Pools and Mobile Pool Groups on the Broadband Gateway on page 230

## Overview of Mobile Pools and Mobile Pool Groups for the Broadband Gateway

---

An important function of the broadband gateway configured as a Gateway GPRS Support Node (GGSN) or Packet Data Network Gateway (P-GW) is to manage IP addresses of subscribers. On the broadband gateway, IP addresses are configured using mobile pools and mobile pool groups, which can contain one or more mobile pools.

A subscriber on the broadband gateway can be assigned an IP address by the authentication, authorization, and accounting (AAA) server, by the Dynamic Host Configuration Protocol (DHCP) server, or locally by the broadband gateway. In addition, a user equipment can provide its IP address (previously assigned by the Home Location Register [HLR]) to the broadband gateway in the Create packet data protocol (PDP) Context or Create Session Request message.

If the gateway assigns the IP address, then the address assignment is called *dynamic*. If the IP address is assigned by an external authority (AAA server, DHCP server, or statically by the user equipment), then the address assignment is called *external*. When the user equipment provides the IP address to the gateway, this type of external address assignment is further classified as *static*. In all these cases, except when addresses are assigned by the DHCP server, the IP addresses must be configured on the broadband gateway in a mobile pool; if an IP address is not configured on the gateway, then the subscriber session is rejected.

Mobile pools, also called mobile address pools, contain a set of IP addresses specified by network prefixes, and are configured under a routing instance. You can configure more than one set of addresses in a mobile pool and restrict the address ranges from which IP addresses are allocated within the mobile pool. In addition to configuring IP addresses in a mobile pool, you can also configure other parameters related to address assignment; for example, you can indicate that the addresses in a mobile pool are assigned externally, or that the pool is a default pool, and so on. You can configure mobile pools to contain IPv4 addresses or IPv6 addresses, but not both.

The broadband gateway also allows you to collect one or more mobile pools into a mobile pool group. All the mobile pools in a mobile pool group should be of the same protocol family: `inet` or `inet6`. In addition, none of the mobile pools in a mobile pool group should be marked as a default. If the gateway assigns addresses locally using a mobile pool group, then the addresses are assigned from the mobile pools that constitute the mobile pool group. Mobile pool groups provide redundancy for IP address assignment.

Mobile pool groups or mobile pools, *except* default mobile pools, can then be added to an access point name (APN). Default mobile pools are used by APNs when no pool has been added to an APN. The address assignment configuration on the APN determines the method by which IP addresses are assigned to subscribers.

**Related  
Documentation**

- *address-assignment (APN)*
- *address-assignment (MobileNext Broadband Gateway)*
- [Configuring Address Assignment on a Broadband Gateway APN on page 122](#)
- [Configuring Mobile Pools and Mobile Pool Groups on the Broadband Gateway on page 230](#)
- [Example: Simple Unified Edge Configuration on page 651](#)

---

## Configuring Mobile Pools and Mobile Pool Groups on the Broadband Gateway

On the broadband gateway configured as a Gateway GPRS Support Node (GGSN) or Packet Data Network Gateway (P-GW), subscriber IP addresses are configured using mobile pools and mobile pool groups. Mobile pools contain a set of IP addresses, and mobile pool groups are a collection of one or more mobile pools. You can configure both IPv4 and IPv6 mobile pools and mobile pool groups.

To configure mobile pools and mobile pool groups on the broadband gateway:



**NOTE:** The following configuration steps are valid at the `[edit access]` and `[edit routing-instances instance-name access]` hierarchy levels. However, for clarity, they are presented only at the `[edit access]` hierarchy level.

- 
1. Specify that you want to configure mobile pools and mobile pool groups.

```
[edit access]
user@host# edit address-assignment
```

2. Specify a name for the mobile pool.

```
[edit access address-assignment]
user@host# set mobile-pools name
```

The pool name can contain letters, numbers, and hyphens (-) and can be up to 63 characters long.

3. Specify the protocol family (`inet` for IPv4 addresses and `inet6` for IPv6 addresses) for the mobile pool named `mbg-pool1`.

```
[edit access address-assignment]
user@host# set mobile-pools mbg-pool1 family (inet | inet6)
```



**NOTE:** A mobile pool must have the protocol family configured.

For example, to configure a mobile pool with IPv4 addresses:

```
[edit access address-assignment]
user@host# set mobile-pools mbg-pool1 family inet
```

4. Specify the network prefix for the mobile pool for the configured protocol family.

```
[edit access address-assignment]
user@host# set mobile-pools mbg-pool1 family inet network [network-prefix]
```



**NOTE:** A mobile pool must have at least one network prefix configured. You can configure more than one network prefix by including the `network` statement multiple times.

For example, to configure a mobile pool with network prefixes 100.100.0.0/16 and 200.200.0.0/16:

```
[edit access address-assignment]
user@host# set mobile-pools mbg-pool1 family inet network 100.100.0.0/16
user@host# set mobile-pools mbg-pool1 family inet network 200.200.0.0/16
```

5. (Optional) Configure the prefix length for address allocation in mobile pools. The allocation prefix length determines the size of the address allocation block (or chunk) assigned to each session PIC on the broadband gateway.

```
[edit access address-assignment]
user@host# set mobile-pools mbg-pool1 family inet network [network-prefix]
allocation-prefix-length allocation-prefix-length
```



**NOTE:**

- If you configure the allocation prefix length, then you cannot configure the `external-assigned` statement.
- The allocation prefix length cannot be less than the corresponding network prefix length. For example, if the network prefix length is 24 (for IPv4), the allocation prefix length cannot be 23 or 22.

The default allocation prefix length is 22 (1024 addresses) for IPv4, and 54 (1024 addresses) for IPv6. The range is 32 (1 address) to 22 (1024 addresses) for IPv4 addresses, and 64 (1 address) to 54 (1024 addresses) for IPv6 addresses.

6. Optionally, specify that the addresses in the configured network prefix are assigned by an external authority; for example, by the authentication, authorization, and accounting (AAA) server or statically by the user equipment.

```
[edit access address-assignment]
```

```
user@host# set mobile-pools mbg-pool1 family inet network [network-prefix]
external-assigned
```



**NOTE:** If you configure the `external-assigned` statement, then you cannot configure the `allocation-prefix-length` statement.

7. (Optional) Specify the address ranges within the network prefix of the mobile pool. If a range is specified, then the broadband gateway assigns IP addresses only from the specified range.

```
[edit access address-assignment]
user@host# set mobile-pools mbg-pool1 family inet network [network-prefix] range
name low low high high
```

For example, to specify an address range starting from 100.0.0.2 and ending with 100.0.0.32:

```
user@host# set mobile-pools mbg-pool1 family inet network 100.100.0.0/16 range r1
low 100.0.0.2 high 100.0.0.32
```



**NOTE:**

- The range name can contain letters, numbers, and hyphens (-) and can be up to 63 characters long.
- You can specify more than one range for a mobile pool. However, within a pool the name of the range must be unique.
- If you specify a range, then you must specify both an upper address (IPv4) or prefix (IPv6) and a lower address (IPv4) or prefix (IPv6) for that range.

- a. (Optional) Specify that the addresses in the configured range are assigned by an external authority.

```
[edit access address-assignment]
user@host# set mobile-pools mbg-pool1 family inet network [network-prefix] range
name external-assigned
```



**NOTE:** If you configure the `external-assigned` statement, then you cannot configure the `allocation-prefix-length` statement.

8. (Optional) Configure the time, in seconds, up to which IP addresses from the mobile pool are not reused. Addresses from deleted packet data protocol (PDP) contexts or bearers are not reused by the broadband gateway until the configured time elapses.

```
[edit access address-assignment]
user@host# set mobile-pools mbg-pool1 ageing-window ageing-window
```

The default ageing window is 2 seconds, and the range is 1 through 65,535 seconds.

9. (Optional) Specify that the mobile pool is a default pool. The broadband gateway uses the default pool to assign IP addresses to subscribers when a mobile pool or

mobile pool group is not explicitly specified in the address assignment configuration for the access point name (APN).

```
[edit access address-assignment]
user@host# set mobile-pools mbg-pool1 default-pool
```

10. (Optional) Specify the pool usage threshold in the mobile pool for pre-fetching addresses. The pre-fetch threshold is used when the mobile pool is configured with prefixes, and when prefixes are added to an existing pool.

```
[edit access address-assignment]
user@host# set mobile-pools mbg-pool1 pool-prefetch-threshold
pool-prefetch-threshold
```

The default pre-fetch threshold is 80, and the range is 1 through 100.

11. (Optional) Specify the pool usage threshold in the mobile pool for generating SNMP traps. When the percentage of addresses used in the mobile pool exceeds the specified threshold, a notification is sent indicating that the specified threshold has been crossed. After reaching the specified threshold, when the percentage of addresses used in the mobile pool drops 20 percent below the threshold, the notification indicating that the specified threshold was exceeded is cleared.

```
[edit access address-assignment]
user@host# set mobile-pools mbg-pool1 pool-snmp-trap-threshold
pool-snmp-trap-threshold
```

The default SNMP trap threshold is 80, and the range is 1 through 100.

12. Configure a mobile pool group, which is a collection of one or more mobile pools.

```
[edit access address-assignment]
user@host# set mobile-pool-groups name pool-name
```

The mobile pool group name can contain letters, numbers, and hyphens (-) and can be up to 63 characters long.

For example, to configure a mobile pool group named v4-group with mobile pools v4-pool-1 and v4-pool-2:

```
[edit access address-assignment]
user@host# set mobile-pool-groups v4-group v4-pool-1
user@host# set mobile-pool-groups v4-group v4-pool-2
```



#### NOTE:

- The mobile pools that you specify must be previously configured on the broadband gateway in the same routing instance as the mobile pool group.
- All the mobile pools in a mobile pool group should be of the same protocol family: inet or inet6.
- None of the mobile pools in a mobile pool group should be marked as the default.

**Related  
Documentation**

- *address-assignment (APN)*
- *address-assignment (MobileNext Broadband Gateway)*
- [Configuring Address Assignment on a Broadband Gateway APN on page 122](#)
- [Example: Simple Unified Edge Configuration on page 651](#)
- [Overview of Mobile Pools and Mobile Pool Groups for the Broadband Gateway on page 229](#)



## CHAPTER 11

# Configuring DHCP

- [DHCP Overview on page 235](#)
- [Understanding DHCP Proxy Clients on page 236](#)
- [Configuring DHCPv4 Proxy Client Profiles on page 237](#)
- [Configuring DHCPv6 Proxy Client Profiles on page 240](#)
- [Configuring the DHCP Proxy Client on the Broadband Gateway on page 242](#)
- [Configuring DHCP Traceoptions on the Broadband Gateway on page 242](#)
- [Enabling DHCP on a Broadband Gateway APN on page 245](#)

## DHCP Overview

---

The Dynamic Host Configuration Protocol (DHCP) is an automatic configuration protocol on IP networks, which eliminates the need for intervention by a network administrator. Networks and devices connected to IP networks must be configured before they can communicate with other devices on the network. The DHCP server maintains a database that helps track devices that have been connected to the network, preventing two devices from accidentally being configured with the same IP address.

The IP address is the most important configuration parameter of DHCP. A device must be initially assigned a specific IP address that is appropriate to the network to which the device is attached, and that IP address must not be assigned to any other device on that network. If you move a device to a new network, it must be assigned a new IP address for the new network. You can use the DHCP to manage these assignments automatically. DHCP provides two primary functions:

- Allocating temporary or permanent IP addresses to clients
- Storing, managing, and providing client configuration parameters

A DHCP client contacts a DHCP server for configuration parameters. The DHCP server is typically centrally located and operated by the network administrator. The server is run by a network administrator so that DHCP clients can be reliably and dynamically configured with parameters appropriate to the current network architecture.

You can configure the MobileNext Broadband Gateway to support the following DHCP features:

- DHCP configuration under an access point name (APN)

- DHCP profile configuration

**Related Documentation**

- [Configuring the DHCP Proxy Client on the Broadband Gateway on page 242](#)
- [Enabling DHCP on a Broadband Gateway APN on page 245](#)
- [Understanding DHCP Proxy Clients on page 236](#)

## Understanding DHCP Proxy Clients

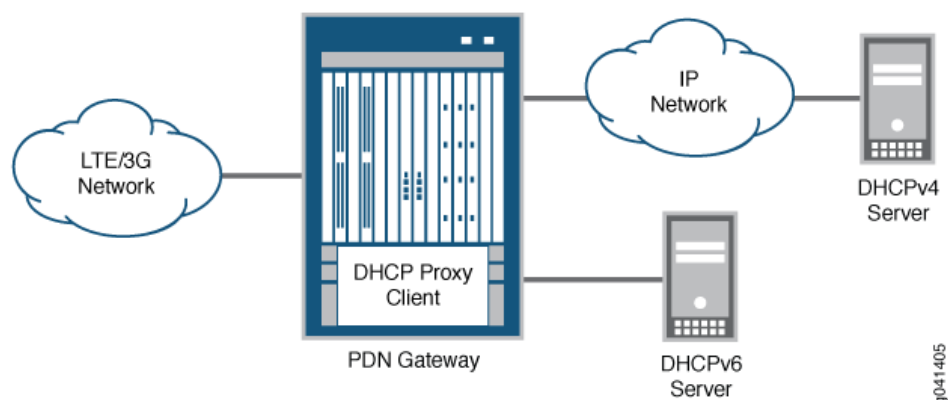
In a typical Dynamic Host Configuration Protocol (DHCP) client configuration, the client and server are on the same subnet. The client requests from the server an IP address and other configuration items and associates them with the local host interface. The association takes place at boot time, at renewal time, or at interface initialization.

On the broadband gateway configured as a Gateway GPRS Support Node (GGSN) or Packet Data Network Gateway (P-GW), DHCP proxy clients enable DHCP-based address allocation for mobile subscribers. The DHCP proxy client acquires a subnet or a prefix from the DHCP server as per DHCP Internet Engineering Task Force (IETF) specifications. The DHCP proxy client then manages the subnet or prefix locally for the mobile subscriber.

The broadband gateway assigns an IP address to the subscriber (from the subnet or prefix obtained from the DHCP server) when a Create PDP Context Request or a Create Session Request is received for that subscriber. When all mobile subscribers using the IP addresses in the subnet or prefix are detached from the broadband gateway, the acquired subnet or prefix is released and the DHCP server can assign the subnet or prefix to another GGSN or P-GW.

[Figure 38 on page 236](#) displays the broadband gateway DHCP proxy client architecture.

**Figure 38: DHCP Proxy Client Architecture**



**Related Documentation**

- [Configuring the DHCP Proxy Client on the Broadband Gateway on page 242](#)
- [\*dhcp-proxy-client\*](#)
- [DHCP Overview on page 235](#)

## Configuring DHCPv4 Proxy Client Profiles

Dynamic Host Configuration Protocol (DHCP) proxy clients enable DHCP-based address allocation for mobile subscribers. On the broadband gateway configured as a Gateway GPRS Support Node (GGSN) or Packet Data Network Gateway (P-GW), you configure a DHCPv4 proxy client profile, which can then be referenced by an access point name (APN) to obtain the subnets from the DHCP server.

To configure a DHCPv4 proxy client profile on the broadband gateway:

1. Specify a name for the DHCPv4 proxy client profile.

```
[edit routing-instances name system services]
[edit system services]
user@host# edit dhcp-proxy-client dhcpv4-profiles profile-name
```

2. Specify the interface on which the DHCPv4 proxy client communicates with the configured DHCP servers. The primary IPv4 address of the bind interface is the source interface of DHCP control packets for DHCPv4.

```
[edit routing-instances name system services dhcp-proxy-client dhcpv4-profiles
profile-name]
[edit system services dhcp-proxy-client dhcpv4-profiles profile-name]
user@host# set bind-interface interface-name
```

For example, to configure ge-1/1/3.0 as the bind interface in a DHCPv4 proxy client profile named dhcpv4-juniper:

```
[edit routing-instances name system services dhcp-proxy-client dhcpv4-profiles
dhcpv4-juniper]
[edit system services dhcp-proxy-client dhcpv4-profiles dhcpv4-juniper]
user@host# set bind-interface ge-1/1/3.0
```



**NOTE:** You must specify a bind interface for the DHCPv4 proxy client profile.

The interface specified here must be previously configured with the valid inet address and inet family at the [edit interfaces] hierarchy level.

3. (Optional) Configure the number of seconds before the broadband gateway reconnects with a dead server that was marked down in previous attempts. A server is marked down if there is no response for multiple successive attempts. The number of attempts can be configured using the **dead-server-successive-retry-attempt** statement.

```
[edit routing-instances name system services dhcp-proxy-client dhcpv4-profiles
profile-name]
[edit system services dhcp-proxy-client dhcpv4-profiles profile-name]
user@host# set dead-server-retry-interval interval-in-seconds
```

The range for the dead server retry interval is 300 through 3600 seconds, and the default is 300 seconds.

4. (Optional) Specify the number of successive retry attempts that the broadband gateway makes to contact a server before declaring an unresponsive server dead. If

a server is marked dead, no DHCP packets are sent to the server until the dead timer, specified using the **dead-server-retry-interval** statement, elapses and the server comes alive.

```
[edit routing-instances name system services dhcp-proxy-client dhcpv4-profiles
  profile-name]
[edit system services dhcp-proxy-client dhcpv4-profiles profile-name]
user@host# set dead-server-successive-retry-attempt number-of-attempts
```

The range for the number of successive retry attempts is 5 through 100, and the default is 10.

5. (Optional) Specify the algorithm used to select the DHCP server with which to communicate when multiple servers are configured.

```
[edit routing-instances name system services dhcp-proxy-client dhcpv4-profiles
  profile-name]
[edit system services dhcp-proxy-client dhcpv4-profiles profile-name]
user@host# set dhcp-server-selection-algorithm (highest-priority-server | round-robin)
```

If the algorithm specified is **highest-priority-server**, then the server with the highest priority is selected. (The server priority is configured using the **priority** statement at the **[edit routing-instances *name* system services dhcp-proxy-client dhcpv4-profiles *name* servers address]** hierarchy level.)

If the algorithm specified is **round-robin**, then the server is selected in a fixed cyclical order. If no algorithm is specified, then the **round-robin** algorithm is used by default.

6. (Optional) Configure the default lease time, in seconds. (The lease time indicates the time for which the broadband gateway holds the DHCP subnets, if the server does not respond to a renewal request. After the lease time elapses, the subnets are removed from the gateway and the subscriber is deleted. If the DHCP client does not get the lease time from the DHCP server, it uses the configured default lease time as the lease time.)

```
[edit routing-instances name system services dhcp-proxy-client dhcpv4-profiles
  profile-name]
[edit system services dhcp-proxy-client dhcpv4-profiles profile-name]
user@host# set lease-time time-in-seconds
```

The range for the default lease time is 60 through 1000 seconds.



**NOTE:** If the DHCP proxy client does not get the lease time from the DHCP server, and if you have not included the **lease-time** statement, then the gateway holds on to the subnets as long as the subscribers, whose addresses are allocated from the subnets, are active. The gateway does not renew the subnets until the DHCP server sends a **FORCE RENEW** message.

7. (Optional) Specify a name for the DHCP server address pool. The broadband gateway requests the DHCP server for a subnet from the configured pool name. The specified pool name is sent to the DHCP server in the DHCP Discover and Request message in **subnet-name-suboption** of **subnet-allocation-option**.

```
[edit routing-instances name system services dhcp-proxy-client dhcpv4-profiles
profile-name]
[edit system services dhcp-proxy-client dhcpv4-profiles profile-name]
user@host# set pool-name pool-name
```

8. (Optional) Configure the maximum number of times that the DHCP proxy client attempts to communicate with the unresponsive DHCP server before the subnet allocation request is deemed as failed.

```
[edit routing-instances name system services dhcp-proxy-client dhcpv4-profiles
profile-name]
[edit system services dhcp-proxy-client dhcpv4-profiles profile-name]
user@host# set retransmission-attempt number-of-attempts
```

The range for the retransmission attempts is 0 through 1000 and the default is 4.

9. (Optional) Configure the amount of time that must pass with no response before the DHCP proxy client reattempts to communicate with the DHCP server.

```
[edit routing-instances name system services dhcp-proxy-client dhcpv4-profiles
profile-name]
[edit system services dhcp-proxy-client dhcpv4-profiles profile-name]
user@host# set retransmission-interval interval-in-seconds
```

The range for the retransmission interval is 4 through 64 seconds, and the default is 4 seconds.

10. Configure the list of DHCP servers with which the DHCP proxy clients communicate to obtain the IPv4 subnet, which is used to allocate IP addresses to mobile subscribers on the broadband gateway.

```
[edit routing-instances name system services dhcp-proxy-client dhcpv4-profiles
profile-name]
[edit system services dhcp-proxy-client dhcpv4-profiles profile-name]
user@host# set servers ip-address
```



**NOTE:** You must configure at least one server. To configure more than one server, include the `servers` statement multiple times.

- a. (Optional) Configure the DHCP server priority. If the algorithm for server selection is based on the highest priority, then the broadband gateway uses the configured priority to select the active server with the highest priority. The DHCP Discover message is then sent to the selected server.

```
[edit routing-instances name system services dhcp-proxy-client dhcpv4-profiles
profile-name]
[edit system services dhcp-proxy-client dhcpv4-profiles profile-name]
user@host# set servers ip-address priority server-priority
```

The range for the priority is 1 (highest priority) to 5 (lowest priority), and the default is 3.

#### Related Documentation

- [Configuring the DHCP Proxy Client on the Broadband Gateway on page 242](#)
- [dhcpv4-profiles](#)

- *dhcpv4-proxy-client-profile* (APN Address Assignment)
- [Understanding DHCP Proxy Clients on page 236](#)

## Configuring DHCPv6 Proxy Client Profiles

---

Dynamic Host Configuration Protocol (DHCP) proxy clients enable DHCP-based address allocation for mobile subscribers. On the broadband gateway configured as a Gateway GPRS Support Node (GGSN) or Packet Data Network Gateway (P-GW), you configure a DHCPv6 proxy client profile, which can then be referenced by an access point name (APN) to obtain the prefixes from the DHCP server.

To configure a DHCPv6 proxy client profile on the broadband gateway:

1. Specify a name for the DHCPv6 proxy client profile.

```
[edit routing-instances name system services]
[edit system services]
user@host# edit dhcp-proxy-client dhcpv6-profiles profile-name
```

2. Specify the interface on which the DHCPv6 proxy client communicates with the configured DHCP servers. The primary IPv6 address of the bind interface is the source interface of DHCP control packets for DHCPv6.

```
[edit routing-instances name system services dhcp-proxy-client dhcpv6-profiles
profile-name]
[edit system services dhcp-proxy-client dhcpv6-profiles profile-name]
user@host# set bind-interface interface-name
```

For example, to configure ge-0/1/5.0 as the bind interface in a DHCPv6 proxy client profile named dhcpv6-juniper:

```
[edit routing-instances name system services dhcp-proxy-client dhcpv6-profiles
dhcpv6-juniper]
[edit system services dhcp-proxy-client dhcpv6-profiles dhcpv6-juniper]
user@host# set bind-interface ge-0/1/5.0
```



**NOTE:** You must specify a bind interface for the DHCPv6 proxy client profile.

The interface specified here must be previously configured with the valid inet6 address and inet6 family at the [edit interfaces] hierarchy level.

---

3. (Optional) Configure the default lease time, in seconds. (The lease time indicates the time for which the broadband gateway holds the DHCP prefixes, if the server does not respond to a renewal request. After the lease time elapses, the prefixes are removed from the gateway and the subscriber is deleted. If the DHCP client does not get the lease time from the DHCP server, it uses the configured default lease time as the lease time.)

```
[edit routing-instances name system services dhcp-proxy-client dhcpv6-profiles
profile-name]
[edit system services dhcp-proxy-client dhcpv6-profiles profile-name]
```

```
user@host# set lease-time time-in-seconds
```

The range for the default lease time is 60 through 1000 seconds.



**NOTE:** If the DHCP proxy client does not get the lease time from the DHCP server, and if you have not included the `lease-time` statement, then the gateway holds on to the prefixes as long as the subscribers, whose addresses are allocated from the prefixes, are active. The gateway does not renew the prefixes until the DHCP server sends a **FORCE RENEW** message.

4. (Optional) Specify a name for the DHCP server address pool. The broadband gateway requests the DHCP server for a prefix from the configured pool name. The specified pool name is sent to the DHCP server in the DHCP Discover and Request message in **subnet-name-suboption** of **subnet-allocation-option**.

```
[edit routing-instances name system services dhcp-proxy-client dhcpv6-profiles
  profile-name]
[edit system services dhcp-proxy-client dhcpv6-profiles profile-name]
user@host# set pool-name pool-name
```

5. (Optional) Configure the maximum number of times that the DHCP proxy client attempts to communicate with the unresponsive DHCP server before the prefix allocation request is deemed as failed.

```
[edit routing-instances name system services dhcp-proxy-client dhcpv6-profiles
  profile-name]
[edit system services dhcp-proxy-client dhcpv6-profiles profile-name]
user@host# set retransmission-attempt number-of-attempts
```

The range for the retransmission attempts is 0 through 1000, and the default is 4.

6. (Optional) Configure the amount of time that must pass with no response before the DHCP proxy client reattempts to communicate with the DHCP server.

```
[edit routing-instances name system services dhcp-proxy-client dhcpv6-profiles
  profile-name]
[edit system services dhcp-proxy-client dhcpv6-profiles profile-name]
user@host# set retransmission-interval interval-in-seconds
```

The range for the retransmission interval is 4 through 64, and the default is 4.

#### Related Documentation

- [Configuring the DHCP Proxy Client on the Broadband Gateway on page 242](#)
- [dhcpv6-profiles](#)
- [dhcpv6-proxy-client-profile \(APN Address Assignment\)](#)
- [Understanding DHCP Proxy Clients on page 236](#)

## Configuring the DHCP Proxy Client on the Broadband Gateway

The broadband gateway uses the DHCP proxy client configuration to assign IP addresses to subscribers if the address assignment method configured on the access point name (APN) is DHCP. A DHCP proxy client can be configured with DHCPv4 proxy client profiles, DHCPv6 proxy client profiles, or both DHCPv4 and DHCPv6 proxy client profiles. In addition, DHCP tracing operations can also be configured for the DHCP proxy client.

To configure a DHCP proxy client on the broadband gateway:

1. Configure one or more DHCPv4 proxy client profiles.  
Refer to [“Configuring DHCPv4 Proxy Client Profiles” on page 237](#) for details.
2. Configure one or more DHCPv6 proxy client profiles.  
Refer to [“Configuring DHCPv6 Proxy Client Profiles” on page 240](#) for details.

### Related Documentation

- [Configuring DHCPv4 Proxy Client Profiles on page 237](#)
- [Configuring DHCPv6 Proxy Client Profiles on page 240](#)
- [dhcp-proxy-client](#)
- [Enabling DHCP on a Broadband Gateway APN on page 245](#)
- [Understanding DHCP Proxy Clients on page 236](#)

## Configuring DHCP Traceoptions on the Broadband Gateway

Dynamic Host Configuration Protocol (DHCP) tracing operations record detailed messages about the operation of DHCP services on the MobileNext Broadband Gateway. You can trace various types of DHCP operations such as errors, warnings, configuration events, and other information. You can specify which trace operations are logged by including specific tracing flags and levels.

[Table 36 on page 242](#) describes the DHCP trace flags that you can include at the **[edit system processes dhcp-service traceoptions flag]** hierarchy level.

**Table 36: DHCP Trace Flags**

Flag	Description
all	Trace all operations.
auth	This flag is not used by the broadband gateway.
database	This flag is not used by the broadband gateway.
fwd	This flag is not used by the broadband gateway.
general	This flag is not used by the broadband gateway.



Table 36: DHCP Trace Flags (*continued*)

Flag	Description
<b>ha</b>	This flag is not used by the broadband gateway.
<b>interface</b>	This flag is not used by the broadband gateway.
<b>io</b>	Trace I/O operations.
<b>liveness-detection</b>	This flag is not used by the broadband gateway.
<b>packet</b>	Trace packet decoding operations.
<b>performance</b>	This flag is not used by the broadband gateway.
<b>profile</b>	This flag is not used by the broadband gateway.
<b>rpd</b>	Trace routing protocol process operations.
<b>rtsock</b>	Trace routing socket operations.
<b>session-db</b>	This flag is not used by the broadband gateway.
<b>state</b>	Trace state transition operations.
<b>statistics</b>	Trace statistics operations.
<b>ui</b>	Trace user interface operations.

To configure tracing options for DHCP operations:

1. Specify that you want to configure tracing options for DHCP operations.  

```
[edit system processes dhcp-service traceoptions]
user@host# edit traceoptions
```
2. Configure the filename for the file that receives the output of the tracing operation. All files are placed in the `/var/log` directory.  

```
[edit system processes dhcp-service traceoptions]
user@host# set file filename
```
3. (Optional) Configure the maximum number of trace files.  

```
[edit system processes dhcp-service traceoptions]
user@host# set file files files
```

The range for the number of files is 2 through 1000, and the default is 3.



**NOTE:** If you specify a maximum number of files, you must also specify a filename and a maximum file size.

4. (Optional) Configure the maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB).

```
[edit system processes dhcp-service traceoptions]
user@host# set file size size
```

The range for the number of files is 10 KB through 1 GB, and the default is 128 KB.



**NOTE:** When a trace file (for example, dhcp-log) reaches its maximum size, it is renamed dhcp-log.0, then dhcp-log.1, and so on, until the maximum number of trace files is reached. The oldest archived file is then overwritten.

If you specify a maximum file size, you must also specify a filename and a maximum number of files.

5. (Optional) Specify that lines matching a configured regular expression are logged.

```
[edit system processes dhcp-service traceoptions]
user@host# set file match match
```

6. (Optional) Specify one of the following viewing permissions for the file:

- Restrict access only to the originator of the trace operation.

```
[edit system processes dhcp-service traceoptions]
user@host# set file no-world-readable
```

- Enable unrestricted file access.

```
[edit system processes dhcp-service traceoptions]
user@host# set file world-readable
```

7. Specify the tracing flag. Refer to [Table 36 on page 242](#) for an explanation of the DHCP tracing flags.

```
[edit system processes dhcp-service traceoptions]
user@host# set flag flag
```



**NOTE:** Use care when tracing all operations (all ) on a gateway as this can have a performance impact.

8. (Optional) Specify that remote tracing is disabled.

```
[edit system processes dhcp-service traceoptions]
user@host# set no-remote-trace
```

**Related  
Documentation**

- [DHCP Overview on page 235](#)
- *traceoptions (DHCP)*
- [Understanding DHCP Proxy Clients on page 236](#)

## Enabling DHCP on a Broadband Gateway APN

You can configure a broadband gateway access point name (APN) to assign IP addresses to subscribers using the IP subnet or prefix returned by the Dynamic Host Configuration Protocol (DHCP) server. If this option is configured, then the broadband gateway uses the information configured in the DHCP proxy client profile to obtain the IP subnet or prefix returned by the DHCP server.

To enable DHCP on a broadband gateway APN:

1. Specify that the broadband gateway uses the information configured in the DHCP proxy client profile to obtain the IP subnet or prefix returned by the DHCP server.

```
[edit unified-edge gateways ggsn-pgw gateway-name apn-services apns name
address-assignment]
user@host# set dhcp-proxy-client
```



**NOTE:** If you include the `dhcp-proxy-client` statement, you must configure a DHCPv4 proxy client profile, a DHCPv6 proxy client profile, or both profiles on the APN, depending on the type of addresses that the APN can allocate (configured in the `apn-data-type` statement).

Refer to “[Configuring Address Assignment on a Broadband Gateway APN](#)” on page 122 for details.

2. Optionally, specify that the IP address returned by the AAA server overrides the address from the subnet or prefix returned from the DHCP server. In this case, if the AAA server provides an IP address for the user equipment, then the gateway does not assign an address from the subnet or prefix, which is returned from the DHCP server for the APN.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
address-assignment]
user@host# set dhcp-proxy-client aaa-override
```

### Related Documentation

- *dhcp-proxy-client (APN Address Assignment)*
- [Configuring Address Assignment on a Broadband Gateway APN on page 122](#)
- [Configuring the DHCP Proxy Client on the Broadband Gateway on page 242](#)



# Configuring IPv6 Stateless Address Autoconfiguration Parameters

- [Understanding IPv6 Stateless Address Autoconfiguration Parameters on page 247](#)
- [Configuring IPv6 Router Advertisement Parameters on page 248](#)
- [Example: Configuring IPv6 Router Advertisement Parameters on page 250](#)

## Understanding IPv6 Stateless Address Autoconfiguration Parameters

---

The MobileNext Broadband Gateway supports IPv6 stateless address autoconfiguration and a series of parameters relating to IPv6 router advertisement.

Some of the most important pieces of IPv6 are built into the way the IPv6 protocol handles routers (or, in this case, the broadband gateway). Instead of requiring the user to configure a default router address, as typical in IPv4 configuration, IPv6 lets routers advertise their presence to other devices on the subnet. This allows hosts to choose the router that is most natural for the application.

You can configure several parameters for a gateway that determine how the IPv6 router protocols operate:

- hop limit—The number of hops used in the router advertisements. A value of zero means routers will not readvertise router availability.
- maximum advertisement interval—The maximum interval the router can wait before sending a router advertisement.
- minimum advertisement interval—The minimum interval the router can wait before sending a router advertisement.
- maximum initial advertisement interval—The maximum interval the router can wait between initial router advertisements.
- maximum initial advertisements—The maximum number of initial router advertisements.
- reachable time—The value used in the reachable time field of the router advertisements.
- router lifetime—The value used in the router lifetime field of the router advertisements.
- retransmission timer—The value used in the retransmit timer field of the router advertisements.

- Related Documentation**
- [Configuring IPv6 Router Advertisement Parameters on page 248](#)
  - [Example: Configuring IPv6 Router Advertisement Parameters on page 250](#)

---

## Configuring IPv6 Router Advertisement Parameters

---

You can configure several parameters for the MobileNext Broadband Gateway that determine how the IPv6 router protocols operate:

Before you begin configuring IPv6 protocol parameters on the broadband gateway, you should have done the following:

- Configured the chassis of the broadband gateway
- Configured the interfaces of the broadband gateway
- Configured the general parameters for the broadband gateway

To determine the IPv6 router protocol behavior, you configure a series of related timers and parameters used in the IPv6 header fields at the `[edit unified-edge ggsn-pgw ggsn-pgw-name ipv6-router-advertisement]` hierarchy level. The parameters apply to a particular gateway.

To configure the IPv6 router protocol parameters:

1. Configure the **current-hop-limit**.

```
[edit unified-edge gateways ggsn-pgw MBG1 ipv6-router-advertisement]
user@host# set current-hop-limit 0
```



**NOTE:** You can configure a value from 0 through 3 hops. The default is 0.

2. Configure the **maximum-advertisement-interval**.

```
[edit unified-edge gateways ggsn-pgw MBG1 ipv6-router-advertisement]
user@host# set maximum-advertisement-interval 21600
```



**NOTE:** You can configure a value from 5400 through 21,600 seconds. The default is 21,600 seconds.

3. Configure the **maximum-initial-advertisement-interval**.

```
[edit unified-edge gateways ggsn-pgw MBG1 ipv6-router-advertisement]
user@host# set maximum-initial-advertisement-interval 10
```



**NOTE:** You can configure a value from 10 through 16 seconds. The default is 10 seconds.

4. Configure the **maximum-initial-advertisements**.

```
[edit ggsn-pgw bb-gw-one ipv6-router-advertisement]
user@host# set maximum-initial-advertisements 3
```



**NOTE:** You can configure a value from 2 through 5. The default is 3.

5. Configure the **minimum-advertisement-interval**.

```
[edit unified-edge gateways ggsn-pgw MBG1 ipv6-router-advertisement]
user@host# set minimum-advertisement-interval 16200
```



**NOTE:** You can configure a value from 3600 through 16200 seconds. The default is 16200 seconds.

6. Configure the **reachable-time**.

```
[edit unified-edge gateways ggsn-pgw MBG1 ipv6-router-advertisement]
user@host# set reachable-time 0
```



**NOTE:** You can configure a value from 0 through 3600000 milliseconds. The default is 0 milliseconds.

7. Configure the **retransmission-timer**.

```
[edit unified-edge gateways ggsn-pgw MBG1 ipv6-router-advertisement]
user@host# set retransmission-timer 0
```



**NOTE:** You can configure a value in milliseconds. The default is 0 milliseconds.

8. Configure the **router-lifetime**.

```
[edit unified-edge gateways ggsn-pgw MBG1 ipv6-router-advertisement]
user@host# set router-lifetime 21840
```



**NOTE:** You can configure a value from 5400 through 21840 seconds. The default is 21840 seconds.

#### Related Documentation

- [Understanding IPv6 Stateless Address Autoconfiguration Parameters on page 247](#)
- [Example: Configuring IPv6 Router Advertisement Parameters on page 250](#)

## Example: Configuring IPv6 Router Advertisement Parameters

---

This example shows how to configure IPv6 protocol parameters on the MobileNext Broadband Gateway. Only IPv6 router advertisement parameters are configured.

- [Requirements on page 250](#)
- [Overview on page 250](#)
- [Configuration on page 250](#)
- [Verification on page 251](#)

### Requirements

This example uses the following hardware and software components:

- An MX chassis equipped with session Dense Port Concentrators (DPCs) and three interface Packet Forwarding Engines (housed in DPCs or Modular Port Concentrators [MPCs]).
- Junos OS Mobility package

Before you begin:

- Install the chassis hardware.
- Configure the chassis, as well as interfaces, anchors, and (optionally) redundancy.

### Overview

IPv6 router advertisements and router solicitation packet handling are exceptions to the rule that user packets flow only through interface Packet Forwarding Engine hardware. This example configures parameters for IPv6 router advertisements. All of the statements in this example use the default values.

### Configuration

#### CLI Quick Configuration

The parameters for IPv6 router advertisements are configured by:

```
[edit unified-edge gateways ggsn-pgw MBG1 ipv6-router-advertisement]
set current-hop-limit 2 # All statements use defaults
set maximum-advertisement-interval 21600
set maximum-initial-advertisement-interval 10
set maximum-initial-advertisements 10
set minimum-advertisement-interval 16200
set reachable-time 0
set retransmission-timer 100
set router-lifetime 21840
```

**Results** From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.



For brevity, these **show** command outputs include only the configuration that is relevant to this example.

```
show unified-edge gateways ggsn-pgw MBG1 ipv6-router-advertisement
current-hop-limit 2;
maximum-advertisement-interval 21600;
maximum-initial-advertisement-interval 10;
maximum-initial-advertisements 10;
minimum-advertisement-interval 16200;
reachable-time 0;
retransmission-timer 100;
router-lifetime 21840;
```

After you configure the device, enter **commit** from configuration mode.

## Verification

### Verifying the IPv6 Parameters Configuration

<b>Purpose</b>	Verify that IPv6 header parameters are set and operating.
<b>Action</b>	There is no way to inspect the IPv6 headers internally on the broadband gateway.
<b>Meaning</b>	You must inspect IPv6 router advertisement packets directly to verify configured header field parameters.
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Understanding IPv6 Stateless Address Autoconfiguration Parameters on page 247</a></li><li>• <a href="#">Configuring IPv6 Router Advertisement Parameters on page 248</a></li></ul>



## PART 5

# Diameter Configuration

- [Diameter Overview on page 255](#)
- [Configuring Diameter on page 259](#)



# Diameter Overview

- [Diameter Base Protocol Overview on page 255](#)
- [Overview of Diameter Profiles on page 256](#)

## Diameter Base Protocol Overview

---

The Diameter protocol is defined in *RFC 3588, Diameter Base Protocol*, and provides an alternative to RADIUS that is more flexible and extensible. The Diameter base protocol provides basic services to one or more applications (also called functions), each running in a different Diameter instance. The individual application provides the extended authentication, authorization, and accounting (AAA) functionality. Applications that use Diameter include Gx applications such as the Policy Charging and Control application, and Gy applications such as the Diameter Credit-Control Application.

Diameter peers communicate over a reliable TCP transport layer connection by exchanging Diameter messages that convey status, requests, and acknowledgements by means of standard Diameter attribute-value pairs (AVPs) and application-specific AVPs.

Each Diameter network element can be associated with one or more functions and consists of a prioritized list of peers. Applications typically send requests to a network element rather than to a single peer. The requests are handled by the appropriate peer based on priority. A lower number has a higher priority. For load balancing, peers have the same priority.

From the prioritized list of peers, the peer is selected as follows:

- The available peer with the highest priority (lowest number) is selected. A peer is available when it is in the Open state and does not have an overloaded outgoing queue.
- In the event of a tie, where the priority is the same, peer selection alternates among available peers with the same priority.

If a peer disconnects, all of its outstanding requests are resubmitted to another peer within the same Diameter network element as part of the failover procedure.

Diameter requires you to configure information about the origin node. Every Diameter node requires Origin-Host and Origin-Realm AVP information that is included in all messages originated from this Diameter node. To configure the Diameter Origin-Host prefix and Origin-Realm, include the **host** and **realm** statements at the **[edit access diameter origin]** hierarchy level.

You can configure one or more transports to specify the source address of the transport layer connection. To configure a Diameter transport, include the **transport** statement at the **[edit access diameter]** hierarchy level. Then include the **address** statement at the **[edit access diameter transport *transport-name*]** hierarchy level.

Each Diameter peer is specified by a name. Peer attributes include the address and the destination TCP port used by active connections to this peer. To configure a Diameter peer, include the **peer** statement at the **[edit access diameter]** hierarchy level, and then include the **address** and **connect-actively** statements at the **[edit access diameter peer *peer-name*]** hierarchy level. To configure the active connection, include the **port** and **transport** statements at the **[edit access diameter peer *peer-name* connect-actively]** hierarchy level. The assigned transport identifies the transport layer source address used to establish active connections to the peers.

To configure a Diameter network element, include the **network-element** statement at the **[edit access diameter]** hierarchy level. Include the **function** statement at the **[edit diameter network-element *element-name*]** hierarchy level. Specify the Diameter peers associated with the Diameter network element by including one or more **peer** statements at the **[edit access diameter network-element *element-name*]** hierarchy level. Set the priority for each peer with the **priority** statement at the **[edit access diameter network-element *element-name* peer *peer-name*]** hierarchy level.

**Related Documentation**

- [Configuring Diameter on page 259](#)

---

## Overview of Diameter Profiles

---

The Diameter profile provides network access information for the Diameter application. The Diameter profile specifies prioritized targets, or endpoints, for particular applications. The target specifies the destination realm, network element, and priority associated with the target.

Target selection is based on priority. A lower number has a higher priority. For load balancing, targets have the same priority.

From the prioritized list of targets for a Diameter profile, the target is selected as follows:

- The target with the highest priority (lowest number) is selected.
- In the event of a tie, where the priority is the same, target selection alternates among the peers with the same priority.



**NOTE:** Failover handling depends on what is allowed by the policy for the application. Switching between targets based on priority, such as failing over between primary and secondary online charging servers, only occurs if the failover handling policy allows it.

---

Once configured, the Diameter profiles can be referenced by the Diameter applications. For example, when configuring transport profiles for online charging, you can associate

the configured Diameter profile with the transport profile to interact with the online charging server. Similarly, when configuring profiles for provisioning Policy Charging and Control application rules, you can associate the configured Diameter profile with the policy and charging enforcement function (PCEF) profile to interact with the policy and charging rules function (PCRF).

**Related  
Documentation**

- [Configuring Diameter Profiles on page 266](#)





# Configuring Diameter

- [Configuring Diameter on page 259](#)
- [Configuring the Origin Attributes of the Diameter Instance on page 260](#)
- [Configuring the Diameter Transport on page 260](#)
- [Configuring Diameter Peers on page 261](#)
- [Configuring Diameter Network Elements on page 263](#)
- [Configuring Advertisements in Diameter Messages on page 263](#)
- [Configuring Parameters for Diameter Applications on page 264](#)
- [Tracing Diameter Operations on page 264](#)
- [Configuring Diameter Profiles on page 266](#)
- [Configuring Diameter AVPs for Gy Applications on page 267](#)
- [Configuring Diameter AVPs for Gx Applications on page 269](#)
- [Configuring Diameter Bindings on page 271](#)
- [Example: Configuring Diameter on page 271](#)
- [Example: Configuring Diameter for Load Balancing on page 279](#)

## Configuring Diameter

---

You configure Diameter by specifying the Diameter base protocol and Diameter profiles. The Diameter base protocol configuration includes configuration of the endpoint origin, the transport layer connection, the remote peers, and the network elements. The Diameter profiles are used by the applications to connect to particular endpoints.

To configure Diameter base protocol:

1. Configure the origin realm and origin host of the Diameter instance.  
[See “Configuring the Origin Attributes of the Diameter Instance” on page 260.](#)
2. Configure the Diameter transport layer.  
[See “Configuring the Diameter Transport” on page 260.](#)
3. Configure the Diameter peers.  
[See “Configuring Diameter Peers” on page 261.](#)

4. Configure the Diameter network elements.  
See [“Configuring Diameter Network Elements” on page 263](#).
5. (Optional) Configure trace options for troubleshooting the configuration.  
See [“Tracing Diameter Operations” on page 264](#).

- Related Documentation**
- [Configuring Diameter Profiles on page 266](#)
  - [Diameter Base Protocol Overview on page 255](#)

---

## Configuring the Origin Attributes of the Diameter Instance

You can configure the identifying characteristics of the endpoint node that originates Diameter messages for the Diameter instance. The hostname is supplied as the value for the Origin-Host prefix. The realm is supplied as the value for the Origin-Realm attribute-value pair (AVP).

To configure the origin attributes:

1. Specify the Origin-Host prefix that originates the Diameter message.

```
[edit access diameter origin]
user@host# set host host14
```

2. Specify the realm of the host that originates the Diameter message.

```
[edit access diameter origin]
user@host# set realm juniper.net
```

- Related Documentation**
- [Configuring Diameter on page 259](#)
  - [Diameter Base Protocol Overview on page 255](#)

---

## Configuring the Diameter Transport

You can configure one or more transports for a Diameter instance to set the source IP address for the local connection, and optionally configure a routing instance context. The routing instance for the transport connection must match that for the peer, or a configuration error is reported. Multiple peers can share the same transport.

To configure a transport for a Diameter instance:

1. Configure the transport name.

```
[edit access diameter]
user@host# set transport t1
```

2. Configure the source IP address for the Diameter local transport connection.

```
[edit access diameter transport t1]
user@host# set address 10.9.20.0
```

3. (Optional) Configure a routing instance, to which the address is bound, for the transport.

```
[edit access diameter transport t1]
user@host# set routing-instance ri10
```

**Related  
Documentation**

- [Configuring Diameter on page 259](#)
- [Configuring Diameter Peers on page 261](#)
- [Diameter Base Protocol Overview on page 255](#)

## Configuring Diameter Peers

You can configure the remote peers to which Diameter sends messages. Port 3868 is used for active connections to peers by default.

To configure a remote peer for a Diameter instance:

1. Specify the name of the Diameter peer.

```
[edit access diameter]
user@host# set peer p3
```

2. Specify the address of the Diameter peer.

```
[edit access diameter peer p3]
user@host# set address 192.168.23.10
```

3. Specify the transport that Diameter uses for active connections to the peer.

```
[edit access diameter peer p3]
user@host# set connect-actively transport t6
```

4. (Optional) Specify the port that Diameter uses for active connections to the peer. The default is port 3868.

```
[edit access diameter peer p3]
user@host# set connect-actively port 3868
```

5. (Optional) Specify the time to wait for connection acknowledgment from the peer. The default is 10 seconds.

```
[edit access diameter peer p3]
user@host# set connect-actively timeout 20
```

6. (Optional) Specify the time to wait before trying to reconnect to a peer after receiving a Disconnect-Peer-Request message with the DO\_NOT\_WANT\_TO\_TALK\_TO\_YOU value for the Disconnect-Cause AVP. If you do not set a value, no reconnection attempt is made.

```
[edit access diameter peer p3]
user@host# set connect-actively repeat-timeout 20
```

7. (Optional) Specify the time to wait for a Capabilities-Exchange-Answer message from the peer. The default is 10 seconds.

```
[edit access diameter peer p3]
user@host# set connect-actively capabilities-exchange-timeout 20
```

8. (Optional) Specify the time to wait between connection attempts for this peer. The default is 30 seconds.

```
[edit access diameter peer p3]  
user@host# set connect-actively retry-timeout 20
```

9. (Optional) Specify the time to wait for a Device-Watchdog-Answer message from the peer. The default is 30 seconds.

```
[edit access diameter peer p3]  
user@host# set watchdog-timeout 20
```

10. (Optional) Specify the time to wait in Closing state while disconnecting this peer. The default is 10 seconds.

```
[edit access diameter peer p3]  
user@host# set disconnect-peer-timeout 20
```

11. (Optional) Specify the size of the incoming queue for the peer. The default is 16000. You can specify a smaller value if you want to throttle the peer.

```
[edit access diameter peer p3]  
user@host# set incoming-queue size 17500
```

12. (Optional) Specify the size of the outgoing queue for the peer. The default is 16000. You can specify a smaller value if you want to throttle the peer.

```
[edit access diameter peer p3]  
user@host# set outgoing-queue size 17500
```

13. (Optional) Specify the low watermark of the outgoing queue for the peer. The default is 60 percent. If the queue size descends to the low watermark after reaching the high watermark, the peer becomes available.

```
[edit access diameter peer p3]  
user@host# set outgoing-queue low-watermark 65
```

14. (Optional) Specify the high watermark of the outgoing queue for the peer. The default is 80 percent. If the queue size reaches the high watermark, the peer is marked unavailable and any new messages to the Diameter network element will not be sent to this peer.

```
[edit access diameter peer p3]  
user@host# set outgoing-queue high-watermark 85
```

**Related  
Documentation**

- [Configuring Diameter on page 259](#)
- [Configuring the Diameter Transport on page 260](#)
- [Configuring Diameter Network Elements on page 263](#)
- [Diameter Base Protocol Overview on page 255](#)

## Configuring Diameter Network Elements

---

A Diameter network element (DNE) consists of associated functions and a list of prioritized peers. The functions associate a Diameter application with the network element. The prioritization determines failover or load-balancing behavior for peer selection.

Before you configure Diameter network elements, perform the following task:

- Define the Diameter peers. See [“Configuring Diameter Peers” on page 261](#).

To configure a Diameter network element:

1. Specify the name of the network element.

```
[edit access diameter]
user@host# set network-element dne25
```

2. Associate one or more functions with the network element. All functions are associated by default.

```
[edit access diameter network-element dne25]
user@host# set function dcca-gy
```

3. Associate a Diameter peer with the network element and set the priority for the peer. Peers with the lower priority number have the higher priority for peer selection. Peers with the same priority are load-balancing peers so the peer selection alternates between the two peers.

```
[edit access diameter network-element dne25]
user@host# set peer peer1 priority 1
```

4. (Optional) Associate a Diameter peer with the network element and set the amount of time to wait for a response from this peer before retransmitting the request to another peer. The default is 4 seconds.

```
[edit access diameter network-element dne25]
user@host# set peer peer1 timeout 5
```

### Related Documentation

- [Configuring Diameter on page 259](#)
- [Configuring Diameter Peers on page 261](#)
- [Diameter Base Protocol Overview on page 255](#)

## Configuring Advertisements in Diameter Messages

---

You can configure information advertised in the Capabilities-Exchange-Request or Capabilities-Exchange-Answer messages. This information includes firmware revision, product name, and vendor identification.

To configure the advertisements:

1. (Optional) Specify the value for the Firmware-Revision AVP that is advertised. 0 is the default.

```
[edit access diameter]
user@host# set firmware-revision 5
```

2. (Optional) Specify the value of the Product-Name AVP that is advertised. Juniper Diameter Client is the default.

```
[edit access diameter]
user@host# set product-name Juniper Client
```

3. (Optional) Specify the value of the Vendor-Id AVP that is advertised. 2636 is the default.

```
[edit access diameter]
user@host# set vendor-id 2636
```

- Related Documentation**
- [Configuring Diameter on page 259](#)
  - *firmware-revision*
  - *product-name*
  - *vendor-id*

---

## Configuring Parameters for Diameter Applications

You can configure parameters for Diameter applications, including the maximum number of pending requests.

To configure the parameters for the Diameter application:

1. (Optional) Specify the Diameter application, the Gy application (**dcca-gy**) or the Gx application (**pcc-gx**), for which you want to configure parameters.

```
[edit access diameter]
user@host# set applications dcca-gy
```

2. (Optional) Specify the maximum number of pending requests for the Diameter application. The default is 20000.

```
[edit access diameter applications dcca-gy]
user@host# set maximum-pending-requests 25000
```

- Related Documentation**
- *applications (Diameter)*
  - [Example: Configuring Diameter on page 271](#)

---

## Tracing Diameter Operations

Tracing operations track Diameter operations and record them in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

All log files are located in the **/var/log** directory. You cannot change the directory in which trace files are located. When the trace file reaches its maximum size, a **.0** is appended

to the filename, then a new file is created with a .1, and finally a .2. When the maximum number of trace files is reached, the oldest trace file is overwritten.



**NOTE:** You should use care when tracing Diameter operations because it can have a performance impact.

To configure tracing operations:

1. Specify that you want to configure tracing options for Diameter operations.

```
[edit]
user@host# edit access diameter traceoptions
```

2. (Optional) Configure the name for the file used for the trace output.
3. (Optional) Configure flags to filter the operations to be logged.
4. (Optional) Configure the peer for which you want to trace packets.

The Diameter traceoptions configuration tasks are described in the following topics:

- [Configuring the Trace Log Filename on page 265](#)
- [Configuring the Tracing Flags on page 265](#)
- [Configuring Tracing for a Diameter Peer on page 266](#)

## Configuring the Trace Log Filename

By default, the name of the file that records trace output for Diameter operations is **diameter**. You can specify a different name with the **file** option to distinguish trace output for different session Dense Port Concentrators (DPCs).

To configure the filename for Diameter tracing operations:

- Specify the name of the file used for the trace output.

```
[edit access diameter traceoptions]
user@host# set file filename
```

## Configuring the Tracing Flags

To configure the flags for the events to be logged:

- Configure the flags.

```
[edit access diameter traceoptions]
user@host# set flag flag
```

By default, only important events are logged. You can specify which trace operations are logged by including specific tracing flags. [Table 37 on page 266](#) describes the flags that you can include.

Table 37: Diameter Tracing Flags

Flag	Description
<b>all</b>	Trace all operations
<b>receive</b>	Trace received packets
<b>receive-detail</b>	Trace received packets in detail
<b>send</b>	Trace transmitted packets
<b>send-detail</b>	Trace transmitted packets in detail
<b>state</b>	Trace Diameter peer state changes
<b>timeout</b>	Trace timeout events

## Configuring Tracing for a Diameter Peer

To configure the peer for which packets are traced:

- Configure the peer.  

```
[edit access diameter traceoptions]
user@host# set peer peer-name
```

### Related Documentation

- [Configuring Diameter on page 259](#)

## Configuring Diameter Profiles

The Diameter profile provides network access information for the Diameter application.

To configure the Diameter profile:

1. Create the Diameter profile for the Gy application (**gy-profile**) or for the Gx application (**gx-profile**).

```
[edit]
user@host# set unified-edge diameter-profiles gy-profile gy1
```

2. Set up the target for the profile.

```
[edit unified-edge diameter-profiles gy-profile gy1]
user@host# set targets ocs-dne-primary
```

3. Specify the destination realm associated with the target.

```
[edit unified-edge diameter-profiles gy-profile gy1 targets ocs-dne-primary]
user@host# set destination-realm juniper.net
```

4. Specify the priority associated with the target. The prioritization determines failover or load-balancing behavior. For load balancing, configure the targets with the same priority.



```
[edit unified-edge diameter-profiles gy-profile gy1 targets ocs-dne-primary]
user@host# set priority 1
```

5. Specify the network element associated with the target.

```
[edit unified-edge diameter-profiles gy-profile gy1 targets ocs-dne-primary]
user@host# set network-element ocs-dne1
```

6. (Optional) Specify the destination host associated with the target.

```
[edit unified-edge diameter-profiles gy-profile gy1 targets ocs-dne-primary]
user@host# set destination-host host25
```

#### Related Documentation

- [Configuring Diameter on page 259](#)
- [Configuring Diameter AVPs for Gy Applications on page 267](#)
- [Configuring Diameter AVPs for Gx Applications on page 269](#)
- [Overview of Diameter Profiles on page 256](#)

## Configuring Diameter AVPs for Gy Applications

Diameter attribute-value pairs (AVPs) can be excluded from or included in the Credit Control Request (CCR) messages between the Gateway GPRS Support Node (GGSN) or Packet Data Network Gateway (P-GW) and the Online Charging System (OCS).



**NOTE:** The configuration of the Diameter AVPs for online charging is optional.

To configure Diameter AVPs for online charging:

1. Specify the name of the Diameter Gy profile for which you are configuring the Diameter AVPs.

```
[edit]
user@host# edit unified-edge diameter-profiles gy-profile profile-name
```

The Diameter profile name can contain letters, numbers, and hyphens (-) and can be up to 128 characters long.

2. Specify the optional AVPs to be excluded from the CCR messages between the GGSN or P-GW and the OCS. By default, all AVPs are included in the CCR messages.

```
[edit unified-edge diameter-profiles gy-profile profile-name]
user@host# set attributes exclude [attribute]
```

You can specify more than one AVP in a single line. For example, to exclude all 3GPP AVPs and the PS-Information AVP from the CCR messages:

```
[edit unified-edge diameter-profiles gy-profile profile-name]
user@host# set attributes exclude all-3gpp-avps ps-information
```

[Table 38 on page 268](#) describes the AVPs that can be excluded from CCR messages.

Table 38: Diameter AVP Exclusions for Gy Applications

AVP	Information in AVP
<b>all-3gpp-avps</b>	All 3GPP AVPs under the PS-Information AVP (where PS stands for packet switched).
<b>cc-selection-mode</b>	Charging-Characteristics-Selection-Mode AVP.
<b>dynamic-address-flag</b>	Dynamic-Address-Flag-Extension AVP.
<b>pdn-connection-id</b>	PDN-Connection-ID AVP.
<b>ps-information</b>	PS-Information AVP, which is normally sent in the Service-Information AVP (as mentioned in 3GPP TS 32.299).
<b>qos-information</b>	QoS-Information AVP.
<b>serving-node-type</b>	Serving-Node-Type AVP.
<b>start-time</b>	Start-Time AVP.
<b>stop-time</b>	Stop-Time AVP.
<b>user-equipment-info</b>	User-Equipment-Info AVP.
<b>user-location-information</b>	User-Location-Info AVP.
<b>username</b>	User-Name AVP.

**NOTE:**

- If only **all-3gpp-avps** is configured, then all 3GPP AVPs under the PS-Information AVP are excluded from the PS-Information AVP; however, the PS-Information AVP (excluding the 3GPP AVPs) is still sent in the Service-Information AVP.
- If only **ps-information** is configured, then all the 3GPP AVPs inside the PS-Information AVP are sent in the Diameter Credit Control Request (CCR) message at the command level; however, the PS-Information AVP is not sent.
- If both **all-3gpp-avps** and **ps-information** are configured, then neither the 3GPP AVPs (inside the PS-Information AVP) nor the PS-Information AVP is sent.

3. Specify the optional AVPs to be included in the CCR messages between the GGSN or P-GW and the OCS. By default, all AVPs are included in the CCR messages.

[edit unified-edge diameter-profiles gy-profile *profile-name*]  
 user@host# set attributes include [*attribute*]

You can specify more than one AVP in a single line. For example, to include the Framed-IP-Address and QoS-Information AVPs in the CCR messages:

```
[edit unified-edge diameter-profiles gy-profile profile-name]
user@host# set attributes include framed-ip-address mscq-qos-information
```

Table 39 on page 269 describes the AVPs that can be included in CCR messages.

**Table 39: Diameter AVP Inclusions for Gy Applications**

AVP	Information in AVP
credit-instance-id	Credit-instance-id AVP.
cumulative-used-service-unit	Used-Service-Unit AVP.
framed-ip-address	Framed-IP-Address AVP, which contains the IPv4 address of the PDP context. If this AVP is excluded, then the PDP Address AVP is used instead.
framed-ipv6-prefix	Framed-IPv6-Prefix AVP.
gprs-negotiated-qos	GPRS Negotiated QoS AVP, which contains the negotiated QoS parameters. If this AVP is excluded, then the QoS-Information AVP is used instead.
mscc-qos-information	QoS-Information AVP of the Multiple-Services-Credit-Control AVP.
service-start-timestamp	Service-start-timestamp AVP.

**Related Documentation**

- *attributes (Diameter Gy Profiles)*

## Configuring Diameter AVPs for Gx Applications

Diameter attribute-value pairs (AVPs) can be excluded from or included in the Credit Control Request (CCR) messages between the Gateway GPRS Support Node (GGSN) or Packet Data Network Gateway (P-GW) and the Policy and Charging Enforcement Function (PCEF).



**NOTE:** The configuration of the Diameter AVPs for dynamic PCEF policies is optional.

To configure Diameter AVPs for Gx applications:

1. Specify the name of the Diameter Gx profile for which you are configuring the Diameter AVPs.

```
[edit]
user@host# edit unified-edge diameter-profiles gx-profile profile-name
```

The Diameter profile name can contain letters, numbers, and hyphens (-) and can be up to 128 characters long.

- Specify the optional AVPs to be excluded from the CCR messages between the GGSN or P-GW and the PCEF. By default, all AVPs are included in the CCR messages.

```
[edit unified-edge diameter-profiles gx-profile profile-name]
user@host# set attributes exclude [attribute]
```

You can specify more than one AVP in a single line.

[Table 40 on page 270](#) describes the AVPs that can be excluded from CCR messages.

**Table 40: Diameter AVP Exclusions for Gx Applications**

AVP	Information in AVP
<b>an-gw-address</b>	AN-GW-Address AVP, which contains the IP addresses of the access node gateway.
<b>default-eps-bearer-qos</b>	Default-EPS-Bearer-QoS AVP.
<b>packet-filter-information</b>	Packet-Filter-Information AVP.
<b>packet-filter-operation</b>	Packet-Filter-Operation AVP.
<b>rat-type</b>	RAT-Type AVP.

- Specify the optional AVPs to be included in the CCR messages between the GGSN or P-GW and the PCEF. By default, all AVPs are included in the CCR messages.

```
[edit unified-edge diameter-profiles gx-profile profile-name]
user@host# set attributes include [attribute]
```

You can specify more than one AVP in a single line.

[Table 41 on page 270](#) describes the AVPs that can be included in CCR messages.

**Table 41: Diameter AVP Inclusions for Gx Applications**

AVP	Information in AVP
<b>gx-capability-list</b>	Gx-capability-list AVP.
<b>rule-suggestion</b>	Rule-suggestion AVP.

**Related Documentation**

- attributes (Diameter Gx Profiles)*

## Configuring Diameter Bindings

A Diameter network element can be configured to run on a specific session PIC. Other session PICs can be organized in a group around the selected session PIC on which the configured network element runs. When organized in a group, the selected session PIC can send and receive messages for other session PICs in the group. By default, every Diameter network element runs on every session PIC.



**NOTE:** If you want to set up Diameter bindings for session PICs on the broadband gateway, contact Juniper Networks Professional Services for assistance.

To configure the Diameter binding for network elements:

1. Configure the network element used for the Diameter binding on the broadband gateway.

```
[edit]
user@host# set unified-edge ggsn-pgw gateway MBG1 diameter network-element
ocs-dne1
```

2. Specify the session PICs group that serves the network element.

```
[edit unified-edge ggsn-pgw gateway MBG1 diameter network-element ocs-dne1]
user@host# set session-pics group bg1
```

3. Specify the session PIC interfaces in this group that serve the network element. The interface must be a multiservices interface.

```
[edit unified-edge ggsn-pgw gateway MBG1 diameter network-element ocs-dne1
session-pics group bg1]
user@host# set session-pic ams0
user@host# set session-pic ms-1/1/0
```

**Related Documentation**

- *diameter (GGSN or P-GW)*

## Example: Configuring Diameter

This example shows how to configure Diameter on the MobileNext Broadband Gateway.

- [Requirements on page 271](#)
- [Overview on page 272](#)
- [Configuration on page 272](#)
- [Verification on page 276](#)

## Requirements

This example uses the following hardware and software components:

- Junos OS Release 12.1W

- Juniper Networks MobileNext Broadband Gateway

Before you configure Diameter, make sure you have the following information:

- IP addresses for the Diameter peers
- Source IP address

## Overview

This example describes how to configure Diameter for the broadband gateway, which includes configuring the Diameter Base protocol and the Diameter profiles. You specify the transport and the peers for the Diameter network elements in order to configure the Diameter Base protocol. The Diameter profiles are used to connect network nodes to support functions such as a Gy application. The Diameter profiles reference targets which reference Diameter network elements which reference Diameter peers.

This example configures a Diameter profile for use by a Gy application that supports online charging: the Diameter Credit-Control Application (DCCA).

## Configuration

To configure Diameter, perform these tasks:

- [Configuring Diameter on page 272](#)
- [Configuring Diameter Profiles on page 274](#)

---

### Configuring Diameter

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set access diameter traceoptions file diameter
set access diameter traceoptions file size 4m
set access diameter traceoptions level all
set access diameter traceoptions flag all
set access diameter origin realm juniper.net
set access diameter origin host host1
set access diameter transport trans1 address 99.1.1.1
set access diameter peer ocs1-primary address 10.1.1.1
set access diameter peer ocs1-primary connect-actively transport trans1
set access diameter peer ocs1-primary watchdog-timeout 20
set access diameter peer ocs2-primary address 10.1.1.2
set access diameter peer ocs2-primary connect-actively transport trans1
set access diameter peer ocs2-primary watchdog-timeout 20
set access diameter peer ocs-secondary address 10.1.1.3
set access diameter peer ocs-secondary connect-actively transport trans1
set access diameter peer ocs-secondary watchdog-timeout 20
set access diameter network-element ocs-dne-primary function dcca-gy
set access diameter network-element ocs-dne-primary peer ocs1-primary priority 1
set access diameter network-element ocs-dne-primary peer ocs-secondary priority 2
set access diameter network-element ocs-dne-secondary function dcca-gy
set access diameter network-element ocs-dne-secondary peer ocs2-primary priority 1
set access diameter network-element ocs-dne-secondary peer ocs-secondary priority 2
```

- Step-by-Step Procedure** To configure Diameter, you specify the origin, remote peers, transport, and network elements:
1. Set up the Origin-Host prefix and Origin-Realm attribute for the endpoint that originates Diameter messages.
 

```
[edit]
user@mbg1# set access diameter origin realm juniper.net
user@mbg1# set access diameter origin host host1
```
  2. Specify the local transport name and the source IP address.
 

```
[edit]
user@mbg1# set access diameter transport trans1 address 99.1.1.1
```
  3. Set up the remote peers to which Diameter sends messages.
 

```
[edit ]
user@mbg1# set access diameter peer ocs1-primary address 10.1.1.1
user@mbg1# set access diameter peer ocs1-primary connect-actively transport
trans1
user@mbg1# set access diameter peer ocs1-primary watchdog-timeout 20
user@mbg1# set access diameter peer ocs2-primary address 10.1.1.2
user@mbg1# set access diameter peer ocs2-primary connect-actively transport
trans1
user@mbg1# set access diameter peer ocs2-primary watchdog-timeout 20
user@mbg1# set access diameter peer ocs-secondary address 10.1.1.3
user@mbg1# set access diameter peer ocs-secondary connect-actively transport
trans1
user@mbg1# set access diameter peer ocs-secondary watchdog-timeout 20
```
  4. Specify the network elements with their associated functions and prioritized peers.
 

```
[edit]
user@mbg1# set access diameter network-element ocs-dne-primary function
dcca-gy
user@mbg1# set access diameter network-element ocs-dne-primary peer
ocs1-primary priority 1
user@mbg1# set access diameter network-element ocs-dne-primary peer
ocs-secondary priority 2
user@mbg1# set access diameter network-element ocs-dne-secondary function
dcca-gy
user@mbg1# set access diameter network-element ocs-dne-secondary peer
ocs2-primary priority 1
user@mbg1# set access diameter network-element ocs-dne-secondary peer
ocs-secondary priority 2
```
  5. Specify Diameter tracing operations.
 

```
[edit]
user@mbg1# set access diameter traceoptions file diameter
user@mbg1# set access diameter traceoptions file size 4m
user@mbg1# set access diameter traceoptions level all
user@mbg1# set access diameter traceoptions flag all
```

**Results**    user@mbg1# show access diameter

```
traceoptions {
  file diameter size 4m;
  level all;
  flag all;
}
origin {
  realm juniper.net;
  host host1;
}
network-element ocs-dne-primary {
  function dcca-gy;
  peer ocs1-primary {
    priority 1;
  }
  peer ocs-secondary {
    priority 2;
  }
}
network-element ocs-dne-secondary {
  function dcca-gy;
  peer ocs2-primary {
    priority 1;
  }
  peer ocs-secondary {
    priority 2;
  }
}
transport trans1 {
  address 99.1.1.1;
}
peer ocs1-primary {
  address 10.1.1.1;
  connect-actively {
    transport trans1;
  }
  watchdog-timeout 20;
}
peer ocs2-primary {
  address 10.1.1.2;
  connect-actively {
    transport trans1;
  }
  watchdog-timeout 20;
}
peer ocs-secondary {
  address 10.1.1.3;
  connect-actively {
    transport trans1;
  }
  watchdog-timeout 20;
}
```

---

### Configuring Diameter Profiles

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

[edit]



```

set unified-edge diameter-profiles gy-profile gy targets ocs-dne-primary destination-realm
juniper.net
set unified-edge diameter-profiles gy-profile gy targets ocs-dne-primary priority 1
set unified-edge diameter-profiles gy-profile gy targets ocs-dne-primary network-element
ocs-dne-primary
set unified-edge diameter-profiles gy-profile gy targets ocs-dne-secondary
destination-realm juniper.net
set unified-edge diameter-profiles gy-profile gy targets ocs-dne-secondary priority 2
set unified-edge diameter-profiles gy-profile gy targets ocs-dne-secondary
network-element ocs-dne-secondary

```

### Step-by-Step Procedure

To configure the Diameter profile:

1. Create the Diameter profile called gy for the Gy application.  

```

[edit]
user@mbg1# set unified-edge diameter-profiles gy-profile gy

```
2. Set up the target called ocs-dne-primary for the profile and specify its destination realm, priority, and network element.  

```

[edit unified-edge diameter-profiles gy-profile gy]
user@mbg1# set targets ocs-dne-primary destination-realm juniper.net
user@mbg1# set targets ocs-dne-primary priority 1
user@mbg1# set targets ocs-dne-primary network-element ocs-dne-primary

```
3. Set up the target called ocs-dne-secondary for the profile and specify its destination realm, priority, and network element.  

```

[edit unified-edge diameter-profiles gy-profile gy]
user@mbg1# set targets ocs-dne-secondary destination-realm juniper.net
user@mbg1# set targets ocs-dne-secondary priority 2
user@mbg1# set targets ocs-dne-secondary network-element ocs-dne-secondary

```

**Results**    user@mbg1# show unified-edge diameter-profiles

```
gy-profile {
  gy {
    targets {
      ocs-dne-primary {
        destination-realm juniper.net;
        priority 1;
        network-element ocs-dne-primary;
      }
      ocs-dne-secondary {
        destination-realm juniper.net;
        priority 2;
        network-element ocs-dne-secondary;
      }
    }
  }
}
```

## Verification

- [Verifying Diameter Application Status on page 276](#)
- [Verifying Network Elements on page 276](#)
- [Verifying Peers on page 277](#)

---

### Verifying Diameter Application Status

**Purpose**    Verify the Diameter statistics on the broadband gateway for the application.

**Action**    user@mbg1> show unified-edge ggsn-pgw diameter dcca-gy statistics

```
Gateway: PGW
Total Sessions:          0
                        Requests      Answers
-----
Total                    0            0
Credit Control Initial  0            0
Credit Control Update   0            0
Credit Control Terminate 0            0
Re-Auth                  0            0
Abort Session            0            0
Dropped                  0            0
```

**Meaning**    The `show unified-edge ggsn-pgw diameter dcca-gy statistics` command displays the Diameter statistics for the Gy application.

---

### Verifying Network Elements

**Purpose**    Verify the status and statistics on the broadband gateway for the network elements.

**Action** user@mbg1> show unified-edge ggsn-pgw diameter network-element status

```

DNE : ocs-dne-primary
  PEER : ocs
    FPC/PIC      PEER STATE      WATCHDOG STATE
    0/0          I-Open          okay
    0/1          I-Open          okay

DNE : ocs-dne-secondary
  PEER : ocs
    FPC/PIC      PEER STATE      WATCHDOG STATE
    0/0          Closed          initial
    0/1          Closed          initial

user@mbg1> show unified-edge ggsn-pgw diameter network-element statistics
Name: ocs-dne-primary
  Packets In : 0
  Packets Out : 0
  Request Timeouts : 0
  Request Cancellations : 0
  Credit Control Request Out : 0
  Credit Control Answer In : 0

Name: ocs-dne-secondary
  Packets In : 0
  Packets Out : 0
  Request Timeouts : 0
  Request Cancellations : 0
  Credit Control Request Out : 0
  Credit Control Answer In : 0

```

**Meaning** The `show unified-edge ggsn-pgw diameter network-element status` command displays the status of the network elements, including the state of the peer and the watchdog timer. The `show unified-edge ggsn-pgw diameter network-element statistics` command displays the statistics for the network elements.

### Verifying Peers

---

**Purpose** Verify the status and statistics on the broadband gateway for the peers.

**Action** user@mbg1> show unified-edge ggsn-pgw diameter peer status

## Diameter Peer Status

Name : ocs1-primary

```

FPC/PIC      : 0/0
State        : Closed
State Duration : 00:00:00
Watchdog State : initial
Peer Address  : 10.1.1.2
Peer port     : 3868
Source Address : 12.4.1.1
Source Port   : 0

```

Name : ocs1-primary

```

FPC/PIC      : 0/1
State        : Closed
State Duration : 00:00:00
Watchdog State : initial
Peer Address  : 10.1.1.2
Peer port     : 3868
Source Address : 12.4.1.1
Source Port   : 0

```

## user@mbg1&gt; show unified-edge ggsn-pgw diameter peer statistics

## Peer: ocs1-primary

Request Timeouts:	0	
Request Retransmissions:	0	
Messages	Transmitted	Received
-----		
Total Messages	3979	3979
Credit Control Requests	0	0
Credit Control Answers	0	0
Re-Auth Requests	0	0
Re-Auth Answers	0	0
Abort Session Requests	0	0
Abort Session Answers	0	0
Capability Exchange Requests	2	0
Capability Exchange Answers	0	2
Device Watchdog Requests	0	3977
Device Watchdog Answers	3977	0
Disconnect Peer Requests	0	0
Disconnect Peer Answers	0	0

## Peer: ocs-secondary

Request Timeouts:	0	
Request Retransmissions:	0	
Messages	Transmitted	Received
-----		
Total Messages	0	0
Credit Control Requests	0	0
Credit Control Answers	0	0
Re-Auth Requests	0	0
Re-Auth Answers	0	0
Abort Session Requests	0	0
Abort Session Answers	0	0
Capability Exchange Requests	0	0
Capability Exchange Answers	0	0
Device Watchdog Requests	0	0
Device Watchdog Answers	0	0
Disconnect Peer Requests	0	0
Disconnect Peer Answers	0	0

**Meaning** The **show unified-edge ggsn-pgw diameter peer status** command displays the status of the peers, including the state of the peer, the peer address and port, and the source address and port. The **show unified-edge ggsn-pgw diameter peer statistics** command displays the statistics for the peers.

- Related Documentation**
- [Configuring Diameter on page 259](#)
  - *diameter (MobileNext Broadband Gateway)*
  - *diameter-profiles*
  - [Example: Configuring Diameter for Load Balancing on page 279](#)

---

## Example: Configuring Diameter for Load Balancing

This example shows how to configure Diameter on the MobileNext Broadband Gateway to provide load balancing for Diameter peers.

- [Requirements on page 279](#)
- [Overview on page 279](#)
- [Configuration on page 280](#)

### Requirements

This example uses the following hardware and software components:

- Junos OS Release 12.1W
- Juniper Networks MobileNext Broadband Gateway

Before you configure Diameter, make sure you have the following information:

- IP addresses for the Diameter peers
- Source IP address

### Overview

This example describes how to configure Diameter peers for load balancing on the broadband gateway.

This example configures Diameter profiles for use by Gx and Gy applications that support load balancing for the peers referenced by the Diameter network element for the lower-priority target in the Diameter profiles. You configure the Diameter peers with the same priority so that the Diameter network element uses load balancing for peer selection. The targets for the Gx and Gy profiles reference this Diameter network element so that when the target is selected, the peer selection alternates between these peers.

## Configuration

To configure Diameter, perform these tasks:

- [Configuring Diameter for the Primary Network Elements on page 280](#)
- [Configuring Diameter Profiles on page 283](#)

### Configuring Diameter for the Primary Network Elements

---

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set access diameter origin realm juniper.net
set access diameter origin host host1
set access diameter transport trans1 address 99.1.1.1
set access diameter peer ocs-primary address 10.1.1.1
set access diameter peer ocs-primary connect-actively transport trans1
set access diameter peer backup1 address 10.1.1.2
set access diameter peer backup1 connect-actively transport trans1
set access diameter network-element ocs-dne1 function dcca-gy
set access diameter network-element ocs-dne1 peer ocs-primary priority 1
set access diameter network-element ocs-dne1 peer backup1 priority 2
set access diameter peer pcrf1 address 40.1.1.1
set access diameter peer pcrf1 connect-actively transport trans1
set access diameter peer backup2 address 40.1.1.2
set access diameter peer backup2 connect-actively transport trans1
set access diameter network-element pcrf-dne1 function pcc-gx
set access diameter network-element pcrf-dne1 peer pcrf1 priority 1
set access diameter network-element pcrf-dne1 peer backup2 priority 2
set access diameter network-element backup-dne function [ dcca-gy pcc-gx ]
set access diameter network-element backup-dne peer backup1 priority 1
set access diameter network-element backup-dne peer backup2 priority 1
```

#### Step-by-Step Procedure

To configure Diameter, specify the origin, remote peers, transport, and network elements:

1. Set up the Origin-Host prefix and Origin-Realm attribute for the endpoint that originates Diameter messages.

```
[edit]
user@mbg1# set access diameter origin realm juniper.net
user@mbg1# set access diameter origin host host1
```

2. Specify the local transport name and the source IP address.

```
[edit]
user@mbg1# set access diameter transport trans1 address 99.1.1.1
```

3. Set up the remote peers to which Diameter sends messages for the Gy application.

```
[edit ]
user@mbg1# set access diameter peer ocs-primary address 10.1.1.1
user@mbg1# set access diameter peer ocs-primary connect-actively transport trans1
user@mbg1# set access diameter peer backup1 address 10.1.1.2
user@mbg1# set access diameter peer backup1 connect-actively transport trans1
```

4. Set up the remote peers to which Diameter sends messages for the Gx application.

```
[edit ]
user@mbg1# set access diameter peer pcrf1 address 40.1.1.1
user@mbg1# set access diameter peer pcrf1 connect-actively transport trans1
user@mbg1# set access diameter peer backup2 address 40.1.1.2
user@mbg1# set access diameter peer backup2 connect-actively transport trans1
```

5. Specify the primary network elements with their associated functions and prioritized peers.

```
[edit]
user@mbg1# set access diameter network-element ocs-dne1 function dcca-gy
user@mbg1# set access diameter network-element ocs-dne1 peer ocs-primary
  priority 1
user@mbg1# set access diameter network-element ocs-dne1 peer backup1 priority
  2
user@mbg1# set access diameter network-element pcrf-dne1 function pcc-gx
user@mbg1# set access diameter network-element pcrf-dne1 peer pcrf1 priority 1
user@mbg1# set access diameter network-element pcrf-dne1 peer backup2 priority
  2
```

6. Specify the backup network element with their associated functions and prioritized peers.

```
[edit]
user@mbg1# set access diameter network-element backup-dne function [ dcca-gy
  pcc-gx ]
user@mbg1# set access diameter network-element backup-dne peer backup1 priority
  1
user@mbg1# set access diameter network-element backup-dne peer backup2
  priority 1
```

```
Results user@mbg1# show access diameter
origin {
    realm juniper.net;
    host host1;
}
network-element backup-dne {
    function dcca-gy;
    function pcc-gx;
    peer backup1 {
        priority 1;
    }
    peer backup2 {
        priority 1;
    }
}
network-element ocs-dne1 {
    function dcca-gy;
    peer ocs-primary {
        priority 1;
    }
    peer backup1 {
        priority 2;
    }
}
network-element pcrf-dne1 {
    function pcc-gx;
    peer pcrf1 {
        priority 1;
    }
    peer backup2 {
        priority 2;
    }
}
transport trans1 {
    address 99.1.1.1;
}
peer backup1 {
    address 10.1.1.2;
    connect-actively {
        transport trans1;
    }
}
peer backup2 {
    address 40.1.1.2;
    connect-actively {
        transport trans1;
    }
}
peer ocs-primary {
    address 10.1.1.1;
    connect-actively {
        transport trans1;
    }
}
peer pcrf1 {
    address 40.1.1.1;
    connect-actively {
        transport trans1;
    }
}
```



## Configuring Diameter Profiles

- CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:
- ```
[edit]
set unified-edge diameter-profiles gy-profile gy-profile-1 targets ocs destination-realm
juniper.net
set unified-edge diameter-profiles gy-profile gy-profile-1 targets ocs priority 1
set unified-edge diameter-profiles gy-profile gy-profile-1 targets ocs network-element
ocs-dne1
set unified-edge diameter-profiles gy-profile gy-profile-1 targets ocs-backup
destination-realm juniper.net
set unified-edge diameter-profiles gy-profile gy-profile-1 targets ocs-backup priority 2
set unified-edge diameter-profiles gy-profile gy-profile-1 targets ocs-backup
network-element backup-dne
set unified-edge diameter-profiles gx-profile gx1 targets pcrf destination-realm juniper.net
set unified-edge diameter-profiles gx-profile gx1 targets pcrf priority 1
set unified-edge diameter-profiles gx-profile gx1 targets pcrf network-element pcrf-dne1
set unified-edge diameter-profiles gx-profile gx1 targets pcrf-backup destination-realm
juniper.net
set unified-edge diameter-profiles gx-profile gx1 targets pcrf-backup priority 2
set unified-edge diameter-profiles gx-profile gx1 targets pcrf-backup network-element
backup-dne
```
- Step-by-Step Procedure** To configure the Diameter profile:
1. Create the Diameter profile called `gy-profile-1` for the Gy application.
 

```
[edit]
user@mbg1# set unified-edge diameter-profiles gy-profile gy-profile-1
```
  2. Set up the primary target for the profile used by the Gy application and specify its destination realm, priority, and network element.
 

```
[edit unified-edge diameter-profiles gy-profile gy-profile-1]
user@mbg1# set targets ocs destination-realm juniper.net
user@mbg1# set targets ocs priority 1
user@mbg1# set targets ocs network-element ocs-dne1
```
  3. Set up the secondary target called `ocs-backup` for the profile used by the Gy application and specify its destination realm, priority, and network element.
 

```
[edit unified-edge diameter-profiles gy-profile gy-profile-1]
user@mbg1# set targets ocs-backup destination-realm juniper.net
user@mbg1# set targets ocs-backup priority 2
user@mbg1# set targets ocs-backup network-element backup-dne
```
  4. Create the Diameter profile called `gx1` for the Gx application.
 

```
[edit]
user@mbg1# set unified-edge diameter-profiles gx-profile gx1
```
  5. Set up the primary target for the profile used by the Gx application and specify its destination realm, priority, and network element.
 

```
[edit unified-edge diameter-profiles gx-profile gx1]
user@mbg1# set targets pcrf destination-realm juniper.net
```

```
user@mbg1# set targets pcrf priority 1
user@mbg1# set targets pcrf network-element pcrf-dne1
```

6. Set up the secondary target called pcrf-backup for the profile used by the Gy application and specify its destination realm, priority, and network element.

```
[edit unified-edge diameter-profiles gx-profile gx1]
user@mbg1# set targets pcrf-backup destination-realm juniper.net
user@mbg1# set targets pcrf-backup priority 2
user@mbg1# set targets pcrf-backup network-element backup-dne
```

**Results**

```
user@mbg1# show unified-edge diameter-profiles
gy-profile {
  gy-profile-1 {
    targets {
      ocs {
        destination-realm juniper.net;
        priority 1;
        network-element ocs-dne1;
      }
      ocs-backup {
        destination-realm juniper.net;
        priority 2;
        network-element backup-dne;
      }
    }
  }
}
gx-profile {
  gx1 {
    targets {
      pcrf {
        destination-realm juniper.net;
        priority 1;
        network-element pcrf-dne1;
      }
      pcrf-backup {
        destination-realm juniper.net;
        priority 1;
        network-element backup-dne;
      }
    }
  }
}
```

- Related Documentation**
- [Configuring Diameter on page 259](#)
  - *diameter (MobileNext Broadband Gateway)*
  - *diameter-profiles*
  - [Example: Configuring Diameter on page 271](#)

## PART 6

# GPRS Tunneling Protocol (GTP) Configuration

- [GTP Overview on page 287](#)
- [Configuring GTP on page 301](#)



# GTP Overview

- [GTP Versions and GPRS Interfaces Overview on page 287](#)
- [GPRS Tunneling Protocol \(GTP\) Overview on page 289](#)
- [GTP Path Management Overview on page 290](#)
- [Understanding Path Management on page 291](#)
- [GTP Tunnel Management Overview on page 294](#)
- [Understanding Tunnel Management on page 295](#)
- [Restart Counters Overview on page 297](#)
- [Understanding CSID Signaling on page 298](#)
- [Understanding Tunnel Endpoint Identifiers on page 299](#)
- [Understanding GTP-U Error Data Path on page 300](#)

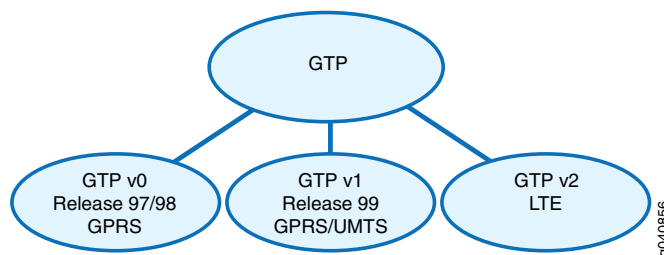
## GTP Versions and GPRS Interfaces Overview

---

The General Packet Radio Service (GPRS) tunneling protocol (GTP) is used to tunnel GTP packets through 3G and 4G networks. A MobileNext Broadband Gateway configured as a gateway GPRS support node (GGSN), Packet Data Network Gateway (P-GW), or GGSN/P-GW automatically selects the appropriate GTP version based on the capabilities of the serving GPRS support node (SGSN) or Serving Gateway (S-GW) to which it is connected.

[Figure 39 on page 287](#) shows the GTP versions that the broadband gateway supports.

**Figure 39: GTP Versions Supported on a MobileNext Broadband Gateway**

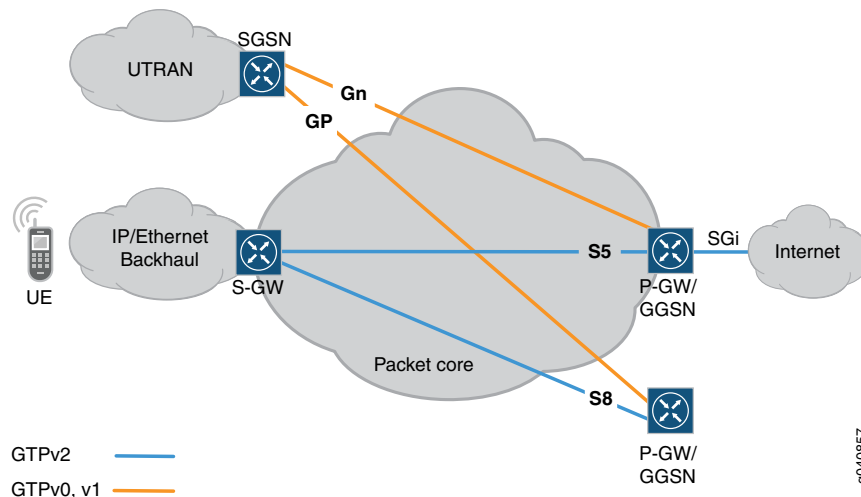


GTP is the primary protocol used in a GPRS core network and allows users in a 3G or 4G network to move from one location to another while remaining connected to the Internet

as if from one location at the GGSN or P-GW by carrying user traffic from the user's current SGSN or S-GW to the GGSN or P-GW that handles the user's session.

Figure 40 on page 288 shows the GTP-C versions the broadband gateway supports for the 3G and 4G network interfaces.

### Figure 40: GTP-C Versions Supported for 3G/4G Network Interfaces



For 3G networks, a broadband gateway uses GTP v0, or GTPv1, or both to transport GTP packets on the GPRS interfaces:

- Gn—The Gn interface is the connection between an SGSN and a GGSN within the same public land mobile network (PLMN).
- Gp—The Gp interface is the connection between two PLMNs.



**NOTE:** GTPv1 is used for both GTP-C and GTP-U. The GTPv1-C protocol runs on UDP port 2123. The GTPv1-U protocol runs on UDP port 2152.

For 4G networks, a broadband gateway uses GTP v2 to transport GTP packets on the GPRS interfaces:

- S5—The S5 interface is the connection between an S-GW and a P-GW within the same PLMN.
- S8—The S8 interface is the connection between two PLMNs.



**NOTE:** The GTPv2 protocol is a control-only protocol and runs on UDP port 2123.

## Related Documentation

- [GPRS Tunneling Protocol \(GTP\) Overview on page 289](#)
- [GTP Tunnel Management Overview on page 294](#)

- [Configuring General GTP Service on the S-GW on page 325](#)

## **GPRS Tunneling Protocol (GTP) Overview**

---

The GPRS Tunneling Protocol (GTP) is the tunneling protocol defined by the 3GPP standards to carry General Packet Radio Service (GPRS) within 3G/4G networks.

GTP is used to establish a GTP tunnel, for user equipment, between a Serving Gateway (S-GW) and Packet Data Network Gateway (P-GW), and an S-GW and Mobility Management Entity (MME). A GTP tunnel is a channel between two GPRS support nodes through which two hosts exchange data. The S-GW receives packets from the user equipment and encapsulates them within a GTP header before forwarding them to the P-GW through the GTP tunnel. When the P-GW receives the packets, it decapsulates them and forwards them to the external host.

GTP comprises the following separate protocols:

- GTP-C— Performs signaling between the S-GW and P-GW in the core GPRS network to activate and deactivate subscriber sessions, adjust the quality of service parameters, or update sessions for roaming subscribers who have arrived from another S-GW. GTP-C supports transport of control packets in IPv4 format.
- GTP-U— Transports user data within the core GPRS network and between the Radio Access Network (RAN) and the core network. GTP-U supports IPv4 and IPv6 user data, but transport is IPv4.

### **Related Documentation**

- [Configuring GTP Services Overview on page 302](#)
- [GTP Path Management Overview on page 290](#)
- [GTP Tunnel Management Overview on page 294](#)
- [Configuring General GTP Service on the S-GW on page 325](#)

## GTP Path Management Overview

---

A GPRS tunneling protocol (GTP) path is active only when both the Packet Data Network Gateway (P-GW) and Serving Gateway (S-GW) are active. The MobileNext Broadband Gateway performs the following functions to check that a peer is active:

- If path management is enabled, the broadband gateway sends periodic echo requests to all peers identified in the peer information table.
- When an echo-request message is received from a peer, the broadband gateway sends an echo-response message.
- If a peer does not respond after a specified number of echo requests, the peer is declared down and all subscriber sessions with the peer are brought down.

This topic covers:

- [Default Path Management Configuration on page 290](#)
- [GTP Version Support for Echo Requests and Echo Responses on page 291](#)

## Default Path Management Configuration

When you configure a broadband gateway as a P-GW without explicitly configuring path management, the following options are automatically enabled with their default values:

- **echo-n3-requests**—Specifies the maximum number of times that the gateway attempts to send a echo-request message. The default is 8 times.
- **echo-t3-response**—Specifies the number of seconds that the gateway waits for a response from a peer gateway before sending the next echo-request message. The default is 15 seconds.
- **echo-interval**—Specifies the number of seconds that the gateway waits before resending a signaling-request message after a response to an echo request is received. The default is 60 seconds.

While an echo response from the peer is pending, the broadband gateway does not send new echo requests even if the path management **echo-interval** elapses. This would occur if echo-t3/echo-n3 is greater than the echo interval and the peer does not respond to the echo request.



**NOTE:** The **echo-interval** timer functions independently from the **echo-n3-requests/echo-t3-response** timer.

---

- **path-management**—Specifies whether path management is enabled or disabled on the broadband gateway. By default, control path management is enabled and data path management is disabled.





**NOTE:** If path-management is disabled, the broadband gateway does continue to send echo-response messages to peer-initiated echo-request messages.

## GTP Version Support for Echo Requests and Echo Responses

Echo messages are sent to the peer using the GTP version that the peer supports. A broadband gateway configured as a GGSN, P-GW, or GGSN/P-GW supports sending echo replies to GTPv0, GTPv1, and GTPv2 echo requests from a peer SGSN or S-GW.

### Related Documentation

- [Configuring GTP Services Overview on page 302](#)
- [GTP Tunnel Management Overview on page 294](#)
- [Understanding Tunnel Endpoint Identifiers on page 299](#)
- [Configuring General GTP Service on the S-GW on page 325](#)

## Understanding Path Management

For a GTP path to be active, the Packet Data Network Gateway (P-GW) and its peer Serving Gateway (S-GW) must be active. To determine that a peer gateway is active, the P-GW exchanges echo-request and echo-response messages. The exchange of the echo-request and echo-response messages between a MobileNext Broadband Gateway and an S-GW allows for quick detection if a GTP path failure occurs.

An echo-request sequence begins when the broadband gateway (P-GW) sends an echo-request message to the S-GW and ends when the S-GW sends a corresponding echo-response message back to the broadband gateway. Path failure occurs when the broadband gateway does not receive a response after a certain number of retries, and all subscriber sessions associated with the down peer are deleted.

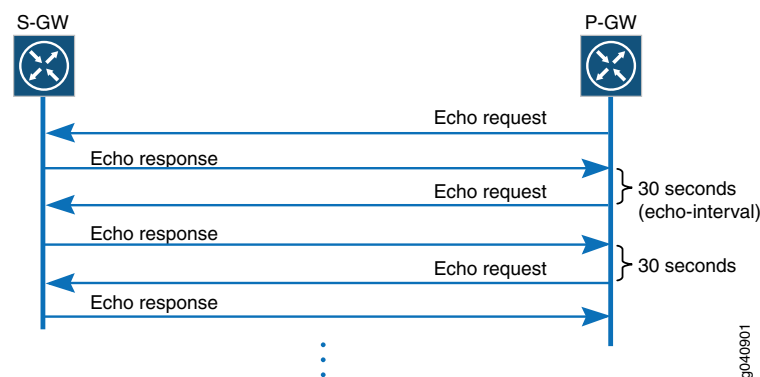
This topic includes the following sections:

- [Successful Echo-Request Sequence for Path Management on page 291](#)
- [Failed Echo Request Sequence for Path Management on page 292](#)

## Successful Echo-Request Sequence for Path Management

In a successful echo-request sequence, the broadband gateway sends an echo-request message to the S-GW and the S-GW sends a corresponding echo-response message back to the broadband gateway, within the configured **echo-n3-requests** and **echo-t3-response** time. [Figure 41 on page 292](#) shows a successful echo-request sequence, in which the P-GW receives an echo response for each echo request.

Figure 41: Successful Echo-Request Sequence for Path Management



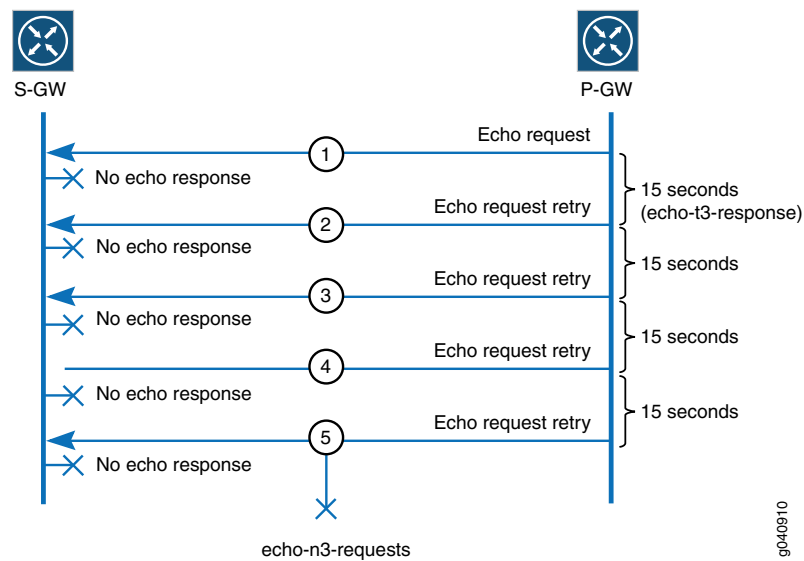
The following steps describe the echo request/response sequence in [Figure 41 on page 292](#):

1. An echo request is sent, and the P-GW receives an echo response within the specified **echo-t3-response** time.
2. The P-GW waits for the configured echo-interval (or default echo-interval of 60 seconds) before sending another echo request, and the P-GW receives an echo response within the specified **echo-t3-response** time.
3. The P-GW waits for the configured echo-interval (or default echo-interval of 60 seconds) before sending another echo request, and the P-GW receives an echo response within the specified **echo-t3-response** time.

### Failed Echo Request Sequence for Path Management

If, after sending a specified number of echo-request messages to the S-GW, the broadband gateway fails to receive a corresponding echo-response message from the S-GW, the GTP path is determined to be down. [Figure 42 on page 293](#) shows a failed echo-request and response sequence in which the P-GW does not receive an echo response within the configured number of **echo-n3-requests** (5 requests) and default **echo-t3-response** time (15 seconds).

### Figure 42: Failed Echo-Request Sequence for Path Management



The following steps describe the echo-request and echo-response sequence in [Figure 42 on page 293](#):

1. The first echo request is sent, but the P-GW does not receive an echo response from the peer within the configured **echo-t3-response** time of 15 seconds.
2. The second echo request is sent, but the P-GW does not receive an echo response within 15 seconds.
3. The third echo request is sent, but the P-GW does not receive an echo response within 15 seconds.
4. The fourth echo request is sent, but the P-GW does not receive an echo response within 15 seconds.
5. The fifth echo request is sent, but the P-GW does not receive an echo response within 15 seconds. At this point, the message flow stops, and the P-GW clears the GTP path and deletes all bearers.

## Related Documentation

- [Configuring GTP Services Overview on page 302](#)
- [GTP Path Management Overview on page 290](#)
- [GTP Tunnel Management Overview on page 294](#)
- [Understanding Tunnel Endpoint Identifiers on page 299](#)
- [Configuring General GTP Service on the S-GW on page 325](#)

## GTP Tunnel Management Overview

---

GTP-C controls and manages tunnels for the nodes connecting to the network in order to establish the user data path. A GTP tunnel is used to deliver packets between the P-GW and S-GW, and is identified in each node by a tunnel endpoint identifier (TEID), an IP address, and a UDP port number. Tunnel management involves creating and deleting end-user sessions and creating, modifying, and deleting bearers during the time a user is connected and using network services.

This tunnel management topic covers:

- [GTP Tunnel Management Functions on page 294](#)
- [Default Tunnel Management Configuration on page 294](#)
- [GTP Version Support for Tunnel Management Requests and Responses on page 294](#)

### GTP Tunnel Management Functions

A broadband gateway provides the following tunnel management functions to manage the GTP tunnel between a GGSN and SGSN or a P-GW and S-GW:

- Send Update bearer request to all peers identified in the Peer Information table.
- Send Delete bearer request to all peers identified in the Peer Information table.
- Send Delete Session request to all peers identified in the Peer Information table.

### Default Tunnel Management Configuration

When you configure a broadband gateway as a P-GW, the tunnel management options are automatically enabled with the following default values:

- **n3-requests**—Specifies the maximum number of times that the gateway attempts to send a Create/Update/Delete tunnel request message. The default is 3 times.
- **t3-response**—Specifies the number of seconds that the gateway waits for a Create/Update/Delete tunnel response from a peer gateway before retransmitting a Create/Update/Delete tunnel request message. The default is 5 seconds.

### GTP Version Support for Tunnel Management Requests and Responses

Create/update/delete tunnel requests are sent to the peer using the GTP version that the peer supports. A broadband gateway configured as a P-GW supports sending Create/Update/Delete responses to GTPv0, GTPv1, and GTPv2 requests from a peer S-GW.

#### Related Documentation

- [Configuring GTP Services Overview on page 302](#)
- [GTP Path Management Overview on page 290](#)
- [Understanding Tunnel Endpoint Identifiers on page 299](#)
- [Configuring General GTP Service on the S-GW on page 325](#)

## Understanding Tunnel Management

You can configure tunnel management on the MobileNext Broadband Gateway to specify the maximum number of request messages to send and how long to wait for a response from a peer before sending a retransmit message.

A tunnel management request-and-response sequence begins when the broadband gateway (P-GW) sends a request message to the S-GW and ends when the S-GW sends a corresponding response message back to the broadband gateway. If the broadband gateway does not receive a response from the S-GW after a certain number of retries, tunnel failure results. When tunnel failure occurs, the broadband gateway deletes the subscriber session associated with the down peer and all Modify or Delete requests associated with that GPRS tunneling protocol (GTP) tunnel.

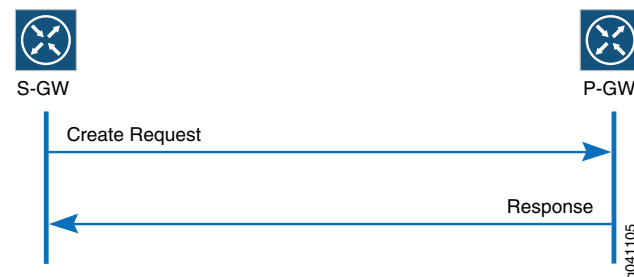
This topic covers:

- [Successful Create Request Sequence for Tunnel Management on page 295](#)
- [Successful Update/Delete Request Sequence for Tunnel Management on page 295](#)
- [Failed Update/Delete Request Sequence for Tunnel Management on page 296](#)

### Successful Create Request Sequence for Tunnel Management

The tunnel management process begins when the Serving Gateway (S-GW) sends a Create request message to the broadband gateway (P-GW), and the broadband gateway sends a corresponding response message back to the S-GW, signaling that the GTP tunnel is active. [Figure 43 on page 295](#) shows a successful Create request sequence in which the S-GW receives a response after sending a request.

**Figure 43: Successful Create Request Sequence for Tunnel Management**



The following steps describe the tunnel management Create request sequence in [Figure 43 on page 295](#):

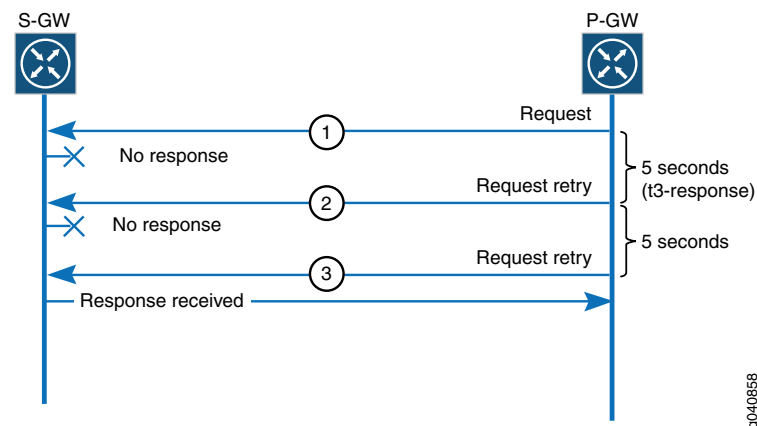
1. The S-GW sends a Create request message to the P-GW.
2. The P-GW sends a response back to the S-GW.

### Successful Update/Delete Request Sequence for Tunnel Management

The tunnel management process begins when the broadband gateway (P-GW) sends an Update or Delete request message to the S-GW, and the S-GW sends a corresponding

response message back to the broadband gateway, signaling that the GTP tunnel is active. [Figure 44 on page 296](#) shows a successful Update or Delete request sequence in which the P-GW receives a response to each request within the specified default values for number of requests and response time.

**Figure 44: Successful Update/Delete Request Sequence for Tunnel Management**



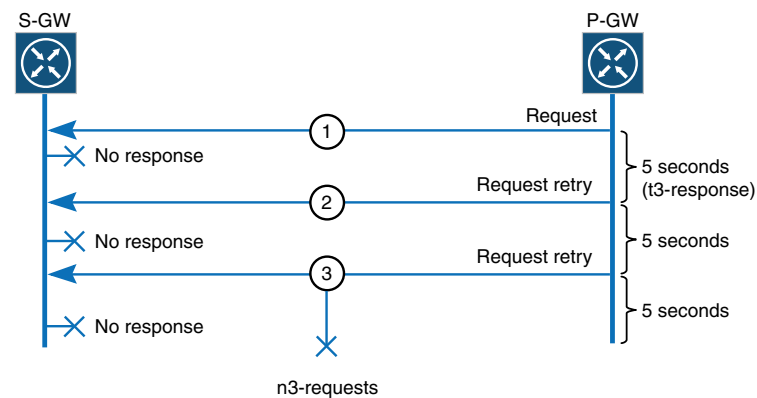
The following steps describe the tunnel management Update or Delete request sequence in [Figure 44 on page 296](#):

1. A request is sent, but the P-GW receives no response within the specified **t3-response** time.
2. A second request is sent, but the P-GW receives no response within the specified **t3-response** time.
3. A third request is sent, and the P-GW receives a response within the specified **t3-response** time.

### Failed Update/Delete Request Sequence for Tunnel Management

If, after sending a specified number of Update or Delete request messages to the S-GW, the broadband gateway fails to receive a corresponding response message from the S-GW, the tunnel path is determined to be down. [Figure 45 on page 297](#) shows a failed tunnel management request sequence in which the P-GW does not receive a response within the specified defaults for number of requests and the response time.

**Figure 45: Failed Update/Delete Request Sequence for Tunnel Management**



g040900

The following steps describe the Update or Delete request failed sequence in [Figure 45 on page 297](#):

1. The first request is sent, but the P-GW receives no response from the peer within the specified **t3-response** time (5 seconds).
2. The second request is sent, but the P-GW receives no response from the peer within the specified **t3-response** time.
3. The third request is sent, but the P-GW receives no response from the peer within the specified **t3-response** time.
4. At this point, the message flow stops, and the P-GW deletes the subscriber session associated with the down peer and all Update or Delete requests associated with that GTP tunnel.

#### Related Documentation

- [Configuring GTP Services Overview on page 302](#)
- [GTP Path Management Overview on page 290](#)
- [GTP Tunnel Management Overview on page 294](#)
- [Understanding Tunnel Endpoint Identifiers on page 299](#)
- [Configuring General GTP Service on the S-GW on page 325](#)

## Restart Counters Overview

The MobileNext Broadband Gateway configured as a P-GW includes the P-GW restart counter (IE) in all GTPv2 messages that it sends to peers. The broadband gateway also receives the S-GW restart counters in GTPv2 messages from the S-GW.

A broadband gateway configured as a P-GW increments the restart counter each time the P-GW is restarted. A broadband gateway receives the peer restart count from the recovery IE in the following GTP-C messages:

- Echo request
- Echo response
- Bearer/PDP context create
- Update messages

A broadband gateway identifies a peer restart by comparing the locally stored peer restart event with the most recent restart count that is received from a peer. If the broadband gateway detects that a peer has restarted by comparing the previously received restart count with the currently received restart count, the broadband gateway deletes all the subscriber sessions associated with the down peer.

**Related  
Documentation**

- [Configuring GTP Services Overview on page 302](#)
- [GTP Path Management Overview on page 290](#)
- [GTP Tunnel Management Overview on page 294](#)
- [Configuring General GTP Service on the S-GW on page 325](#)

---

## Understanding CSID Signaling

---

A Connection Set Identifier (CSID) identifies a group of subscribers and is used during recovery procedures or, when recovery is not possible, to inform peer nodes when a partial failure occurs on the Serving Gateway (S-GW) or Packet Data Network Gateway (P-GW). A *partial failure* is a hardware or software failure that affects a significant number of (but not all) Packet Data Network (PDN) connections. CSIDs are supported on GTPv2 interfaces only.

The CSID can represent a large number of PDN connections within a node (S-GW, P-GW). Each node maintains a local mapping of a CSID to its internal resources. When one or more of those local resources fail, GTPv2 Connection Set Delete request messages send one or more corresponding fully qualified CSIDs to the peer nodes. A fully qualified CSID (FQ-CSID) is the combination of the node identity and the CSID that the node assigns, which together globally identify a set of PDN connections.

A CSID provides notifications based on a set of PDN connections. When the node needs to delete the PDN connections identified by a CSID, the P-GW or S-GW sends a single message to its peers, rather than sending a separate message for each PDN connection. For example, if the S-GW wants to delete a set of PDN connections identified by a CSID, it sends one PDN delete message with FQ-CSID IE (with the value set to CSID) to all connected P-GWs. The receiving P-GWs then delete the PDN connections associated with the received CSID.

**Related  
Documentation**

- [GPRS Tunneling Protocol \(GTP\) Overview on page 289](#)
- [GTP Path Management Overview on page 290](#)
- [GTP Tunnel Management Overview on page 294](#)
- [Understanding Tunnel Endpoint Identifiers on page 299](#)



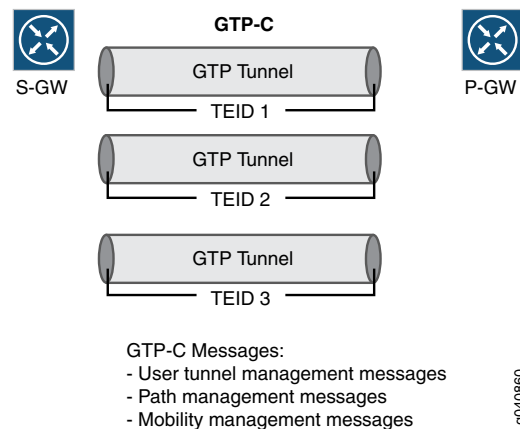
- [Configuring General GTP Service on the S-GW on page 325](#)

## Understanding Tunnel Endpoint Identifiers

The GPRS tunneling protocol (GTP) stack assigns a unique tunnel endpoint identifier (TEID) to each GTP control connection to the peers. The GTP stack also assigns a unique TEID to each GTP user connection (bearer) to the peers. The TEID is a 32-bit number field in the GTP (GTP-C or GTP-U) packet.

[Figure 46 on page 299](#) shows a GTP tunnel with its associated TEID.

**Figure 46: GTP-C Performs Signaling Between the Serving Gateway and Packet Data Network Gateway**



GTP-C allocates a TEID to identify a set of endpoints for a GTP-C tunnel, as shown in [Figure 46 on page 299](#). For each bearer, a separate GTP-U tunnel with its own TEID is established.

An ingress Packet Forwarding Engine performs GTP-C TEID route lookup to identify the target services PIC for the received packet for the following types of GTP-C messages:

- Create PDP context request (for secondary)
- Update PDP context request and response (GTPv1)
- Delete PDP context request and response (GTPv1)
- Create Session response (GTPv2)
- Create bearer request and response (GTPv2)
- Modify bearer request and response (GTPv2)
- Delete Session request and response (GTPv2)
- Delete bearer request and response (GTPv2)

### Related Documentation

- [Configuring GTP Services Overview on page 302](#)
- [GTP Path Management Overview on page 290](#)

- [GTP Tunnel Management Overview on page 294](#)
- [Configuring General GTP Service on the S-GW on page 325](#)

---

## Understanding GTP-U Error Data Path

The MobileNext Broadband Gateway processes GPRS tunneling protocol, user plane (GTP-U) packets with errors in a distinctly different way from non-errored packets, and treats two type of errors differently.

The broadband gateway generates error indications based on two major GTP-U Tunnel Endpoint Identifier (TEID) errors:

- Invalid group TEID
- Invalid TEID

The broadband gateway assigns a TEID to all GTP packets and uses the TEID to associate all traffic belonging to the same tunnel and map one section of a tunnel to another. In addition, TEIDs can be grouped so that all sessions (contexts or bearers) can share the same group TEID for charging or other purposes.

The GTP-U error indication can be caused by an invalid individual or group TEID. In both cases, the session DPC sends the error indication back to the source.

The rate of GTP-U error indications is throttled at all steps to prevent storms of invalid TEID messages.

### Related Documentation

- [Understanding the Broadband Gateway Software Data Path on page 10](#)
- [Understanding IPv6 Stateless Address Autoconfiguration Parameters on page 247](#)
- [Configuring IPv6 Router Advertisement Parameters on page 248](#)
- [Configuring GGSN or P-GW Software Data Path Traceoptions on page 55](#)
- [Configuring S-GW Software Data Path Traceoptions on page 62](#)
- [Example: Configuring IPv6 Router Advertisement Parameters on page 250](#)

# Configuring GTP

- [Configuring GTP Services Overview on page 302](#)
- [Configuring a Loopback Interface for Transport of GTP Packets on page 304](#)
- [Configuring GTP Services on a Broadband Gateway on page 305](#)
- [Configuring GTP Services on the Control Plane on page 306](#)
- [Configuring GTP Services on the Data Plane on page 308](#)
- [Configuring GTP Services on the S5 Interface on page 309](#)
- [Configuring GTP Services on the S8 Interface on page 310](#)
- [Configuring GTP Services on the Gn Interface on page 312](#)
- [Configuring GTP Services on the Gp Interface on page 314](#)
- [Configuring GTP Services When the S5 and S8 Interfaces Are in Different VRFs on page 315](#)
- [Configuring GTP Services When the S5 and S8 Interfaces Are in the Same VRF on page 317](#)
- [Configuring GTP Services When 3GPP Interfaces Are in Different VRFs on page 318](#)
- [Configuring GTP Services on a GGSN Broadband Gateway on page 320](#)
- [Configuring GTP Services on a Peer Group on page 321](#)
- [Disabling Path Management on a Broadband Gateway or Peer Group on page 323](#)
- [Configuring GTP Trace Options on page 323](#)
- [Configuring General GTP Service on the S-GW on page 325](#)
- [Configuring GTP-C Services on the S11 Interface on page 328](#)
- [Configuring GTP-U Services on the S12 Interface on page 330](#)
- [Configuring GTP Services on the S1-U Interface on page 332](#)
- [Configuring GTP Services on the S4 Interface on page 333](#)
- [Configuring GTP Services on the S-GW When the S4 and S5 Interfaces Are in the Same VRF on page 335](#)
- [Configuring GTP Services on the S-GW When Interfaces are in Different VRFs on page 337](#)
- [Configuring S-GW GTP Traceoptions on page 338](#)
- [Example: Configuring GTP for the S-GW When Interfaces Are in different VRFs on page 340](#)

## Configuring GTP Services Overview

---

You can configure GPRS tunneling protocol (GTP) services on a MobileNext Broadband Gateway that is configured as a gateway GPRS support node (GGSN), Packet Data Network Gateway (P-GW), or GGSN/P-GW. At minimum, to configure a broadband gateway requires that you specify a loopback address on which GTP packets for the 3GPP interfaces are received. When configured as a GGSN, a broadband gateway uses only the Gn and Gp interfaces. When configured as a P-GW, a broadband gateway uses only S5 and S8 interfaces. When configured as a GGSN/P-GW, the broadband gateway uses all these 3GPP interfaces: Gn, Gp, S5, and S8.

This topic covers the following:

- [GTP-C and GTP-U Path Management on page 302](#)
- [Configuring GTP Services at Different Levels on a Broadband Gateway on page 302](#)
- [GTP Services Default Settings on page 303](#)
- [GTP Version Support on page 304](#)

### GTP-C and GTP-U Path Management

When you configure a Broadband Gateway, you can specify that GTP-C packets and GTP-U packets are received on different loopback addresses. GTP packets for a GTP-C peer address handle control packets, and GTP packets for a GTP-U peer address handle user (data) packets. Each peer in the GTP path is marked a GTP-C peer or a GTP-U peer, or both.

### Configuring GTP Services at Different Levels on a Broadband Gateway

When you configure a broadband gateway as a GGSN, P-GW, or GGSN/P-GW, GTP services can be configured at the following levels:

- Gateway—The mobile gateway appears as a single address, which comprises a loopback interface/IP address pair, and all GTP packets for the broadband gateway are received on this loopback address.



**NOTE:** To specify a single loopback address on which all GTP packets (GTP-C and GTP-U) are received, the Gn, Gp, S5, and S8 interfaces must be configured in the same VRF routing instance.

---

- Control plane—GTP-C control (signaling) packets are received on a loopback address.

- Data plane—GTP-U data packets are received on a loopback address.
- 3GPP interface—GTP packets transported on the following 3G and 4G interfaces are received on a loopback address:
  - Gn interface—GTP packets on the Gn interface (3G) are received on a single loopback address. Optionally, GTP control or GTP user packets that are transported on the Gn interface also can be received on separate loopback addresses.
  - Gp interface—GTP packets are received on the Gp interface (3G). Optionally, GTP control or user packets that are transported on the Gp interface also can be received on separate loopback addresses.
  - S5 interface—GTP packets are received on the S5 interface (4G). Optionally, GTP control or user packets that are transported on the S5 interface also can be received on separate loopback addresses.
  - S8 interface—GTP packets are received on the S8 interface (4G). Optionally, GTP control or user packets that are transported on the S8 interface also can be received on separate loopback addresses.

If the Gn, Gp, S5, and S8 interfaces for the broadband gateway are each configured in a different Virtual Routing and Forwarding (VRF) routing instance, you must configure GTP services for each interface separately. In this case, each interface (Gn, Gp, S5, and S8) must specify a different loopback interface. In addition, the IP address (that you specify for each loopback interface) must be the same in each VRF because the GTP-C, Mobility Management Entity (MME), and Home Subscriber Server (HSS) applications are not VRF aware and a mobile device could attach from anywhere.

## GTP Services Default Settings

To configure GTP services with all default settings on a P-GW, you can simply configure the loopback address on which GTP packets are received without explicitly configuring any other GTP statements. The GTP defaults configuration is automatically configured on the broadband gateway at the level that you specify the loopback address. For example, the following configuration statement shows a minimum but complete configuration for enabling GTP services on a P-GW:

```
[edit unified-edge mobile gateways ggsn-pgw pgw-1 gtp]
user@host# set interface lo0.0 v4-address 10.10.10.1
```



**NOTE:** If no address is specified for the interface, the broadband gateway uses the default interface IP address, which is configured under interface configuration.

When you do not explicitly configure path management options for GTP services, the broadband gateway uses the defaults, as described in [“GTP Path Management Overview” on page 290](#).

When you do not explicitly configure tunnel management options for GTP services, the broadband gateway uses the defaults, as described in [“GTP Tunnel Management Overview” on page 294](#).

## GTP Version Support

When you configure GTP services on the Broadband Gateway, the type of gateway you configure determines the GTP versions that the broadband gateway supports:

- A broadband gateway configured as a GGSN supports GTPv0 and GTPv1 packets
- A broadband gateway configured as a P-GW supports GTPv2 packets
- A broadband gateway configured as a GGSN/P-GW supports GTPv0, GTPv1, and GTPv2 packets

### Related Documentation

- [GPRS Tunneling Protocol \(GTP\) Overview on page 289](#)
- [GTP Path Management Overview on page 290](#)
- [GTP Tunnel Management Overview on page 294](#)
- [Configuring General GTP Service on the S-GW on page 325](#)

---

## Configuring a Loopback Interface for Transport of GTP Packets

You must configure a loopback interface on an MX Series router before you can configure GTP services for Broadband Gateway.

To configure a loopback interface:

1. Edit the loopback interface.

```
[edit]
user@host# edit interfaces lo0
```

2. Edit the loopback interface unit.

```
[edit interfaces lo0]
user@host# set unit 1
```

3. Edit the loopback interface family.

```
[edit interfaces lo0 unit 1]
user@host# set family inet
```

4. Specify the loopback interface address.

```
[edit interfaces lo0 unit 1 family inet]
user@host# set address 10.10.10.1/32
```

### Related Documentation

- [Configuring GTP Services on a Broadband Gateway on page 305](#)
- [Configuring General GTP Service on the S-GW on page 325](#)

## Configuring GTP Services on a Broadband Gateway

To configure a MobileNext Broadband Gateway as a GGSN/P-GW and enable GTP services, at minimum, you must configure a loopback interface and IP address on which GTP packets are received. Configuring GTP services on the GGSN/P-GW at the data plane, control plane, or (Gn, Gp, S5, or S8) interface level is optional.

The following configuration specifies a loopback address on which all GTP packets are received for the S5, S8, Gn, and Gp interfaces.



**NOTE:** To configure a loopback address on which all GTP packets are received, all 3GPP interfaces (S5, S8, Gn, and Gp) must be in the same VRF.

To configure GTP services on a broadband gateway configured as a GGSN/P-GW:

1. Configure the maximum number of peer entries for which the gateway stores statistics after the peer is deleted.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp]
user@host# set peer-history 1000
```



**NOTE:** In this configuration example, *ggsn-pgw* specifies the gateway personality and *MBG1* is the logical name of the gateway.

2. Configure an IPv4 address on a loopback interface to specify the transport address on which GTP-C and GTP-U packets are received for the S5, S8, Gn, and Gp interfaces.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp]
user@host# set interface lo0.0 v4-address 10.10.10.1
```

3. For tunnel management, configure the maximum number of times that the gateway will attempt to send signaling-request messages to a peer (SGSN or S-GW).

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp]
user@host# set n3-requests 6
```

4. For tunnel management, configure the time that the gateway waits before resending a signaling-request message when a response to the request has not been received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp]
user@host# set t3-response 8
```

5. For path management, configure the maximum number of times that the gateway will attempt to send echo-request messages to a peer (SGSN or S-GW).

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp]
user@host# set echo-n3-requests 6
```

6. For path management, configure the time that the gateway waits before resending an echo-request message when an echo response to the echo request is not received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp]
user@host# set echo-t3-response 4
```

7. For path management, configure the number of seconds that the gateway waits before sending an echo-request message after an echo response is received from the peer.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp]
user@host# set echo-interval 65
```

8. Configure security trace options for the gateway:

- a. Specify a name for the file that receives the output of the tracing operation.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp traceoptions]
user@host# set file gtp_log
```

- b. Configure the maximum size for the trace file.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp traceoptions]
user@host# set size 50m
```

- c. Configure the level of tracing to match all levels, including error conditions, informational messages, notice messages, verbose messages, and warning messages.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp traceoptions]
user@host# set level all
```

- d. Configure the tracing operation to trace all operations.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp traceoptions]
user@host# set flag all
```

**Related  
Documentation**

- [Configuring a Loopback Interface for Transport of GTP Packets on page 304](#)
- [Configuring GTP Services on the Data Plane on page 308](#)
  - [Configuring GTP Services on the Control Plane on page 306](#)
- [Configuring GTP Services Overview on page 302](#)
- [Configuring General GTP Service on the S-GW on page 325](#)

---

## Configuring GTP Services on the Control Plane

To configure a separate address to receive GTP-C packets, you configure services on the router's loopback address. The following configuration specifies an IPv4 transport address on which GTP control packets other than Create Session request are received for the S5, S8, Gn, and Gp interfaces.

To configure GTP services on the control plane for a broadband gateway configured as a GGSN/P-GW:

1. Configure an IPv4 address on a loopback interface to specify the address on which GTP-C packets are received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp control]
user@host# set interface lo0.0 v4-address 10.10.10.1
```



2. For tunnel management, configure the maximum number of times that the gateway will attempt to send signaling-request messages to a peer (SGSN or S-GW).

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp control]  
user@host# set n3-requests 6
```

3. For tunnel management, configure the time that the gateway waits before resending a signaling-request message when a response to the request has not been received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp control]  
user@host# set t3-response 8
```

4. For path management, configure the maximum number of times that the gateway will attempt to send an echo-request message to a peer (SGSN or S-GW).

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp control]  
user@host# set echo-n3-requests 6
```

5. For path management, configure the time that the gateway waits before resending an echo-request message when an echo response to the echo request is not received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp control]  
user@host# set echo-t3-response 4
```

6. For path management, configure the number of seconds that the gateway waits before sending an echo-request message after an echo response is received from the peer.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp control]  
user@host# set echo-interval 65
```

7. Specify a forwarding class for outbound control packets.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp]  
user@host# set forwarding-class assured-forwarding
```

8. Specify a Differentiated Services Code Point (DSCP) value in the IP packet header for outbound control packets.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp]  
user@host# set dscp-code-point 010110
```

#### **Related Documentation**

- [Configuring a Loopback Interface for Transport of GTP Packets on page 304](#)
- [Configuring GTP Services on the Data Plane on page 308](#)
- [Configuring GTP Services on a Broadband Gateway on page 305](#)
- [Configuring GTP Services Overview on page 302](#)
- [Configuring General GTP Service on the S-GW on page 325](#)

## Configuring GTP Services on the Data Plane

---

On a Broadband Gateway, user data is transported through the GTP-U tunnel. To configure a separate address to receive GTP-U packets, you configure services on the router's loopback interface.

The following configuration specifies a separate address on which GTP-U packets are received for the S5, S8, Gn, and Gp interfaces, unless overridden at the 3GPP interface level.

To configure GTP services on the data plane for a broadband gateway configured as a GGSN/P-GW:

1. Configure an IPv4 address on a loopback interface to specify the transport address on which GTP-U packets are received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp data]
user@host# set interface lo0.0 v4-address 10.10.10.1
```

2. For path management, configure the maximum number of times that the gateway will attempt to send an echo-request message to a peer (SGSN or S-GW).

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp data]
user@host# set echo-n3-requests 6
```

3. For path management, configure the time that the gateway waits before resending an echo-request message when an echo response to the echo request is not received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp data]
user@host# set echo-t3-response 4
```

4. For path management, configure the number of seconds that the gateway waits before sending an echo-request message after an echo response is received from the peer.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp data]
user@host# set echo-interval 65
```

5. Configure the number of seconds that the gateway waits before sending a TEID error message to the peer.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp data]
user@host# set error-indication-interval 5
```

### Related Documentation

- [Understanding Tunnel Endpoint Identifiers on page 299](#)
- [Configuring a Loopback Interface for Transport of GTP Packets on page 304](#)
- [Configuring GTP Services on the Control Plane on page 306](#)
- [Configuring GTP Services on a Broadband Gateway on page 305](#)
- [Configuring GTP Services Overview on page 302](#)
- [Configuring General GTP Service on the S-GW on page 325](#)

## Configuring GTP Services on the S5 Interface

The following configuration specifies a separate address on which GTP packets (other than Create Session request) are received for a 3GPP S5 interface.

The address you specify for an S5 interface must be the same address specified for the S8 interface although the VRF can be different. In addition, to allow mobility across 3G and Long Term Evolution (LTE), the S5 address must be the same as Gn and Gp addresses, optionally, with each interface in a different VRF, whether or not these addresses are specified explicitly or implicitly (through inheritance or from a higher level).

To configure GTP services on an S5 interface for a broadband gateway configured as a GGSN/P-GW:

1. Configure an IPv4 address on a loopback interface to specify the transport addresses on which GTP packets on the S5 interface are received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp s5]
user@host# set interface lo0.1 v4-address 10.10.10.1
```

2. For tunnel management, configure the maximum number of times that the gateway will attempt to send signaling-request messages to a peer (SGSN or S-GW).

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp s5]
user@host# set n3-requests 6
```

3. For tunnel management, configure the time that the gateway waits before resending a signaling-request message when a response to the request has not been received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp s5]
user@host# set t3-response 8
```

4. For path management, configure the maximum number of times that the gateway will attempt to send an echo-request message to a peer (SGSN or S-GW).

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp s5]
user@host# set echo-n3-requests 6
```

5. For path management, configure the time that the gateway waits before resending an echo-request message when an echo response to the echo request is not received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp s5]
user@host# set echo-t3-response 4
```

6. For path management, configure the number of seconds that the gateway waits before sending an echo-request message after an echo response is received from the peer.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp s5]
user@host# set echo-interval 65
```

7. To configure a separate address on which GTP control packets are received for the S5 interface:

- a. Configure a loopback address to specify the address on which GTP control packets are received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp s5 control]
```

```
user@host# set interface lo0.6 v4-address 10.10.10.2
```



**NOTE:** The path management and tunnel management configuration you specified at the S5 interface level will also apply to GTP control packets unless you configure path management, or tunnel management, or both at the S5 control level.

- b. To interoperate with older gateways that support a GTP version with 16-bit sequence-number-length, configure the following option.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp s5 control]  
user@host# set sequence-number-length 16-bits
```

- c. Specify a forwarding class for outbound control packets.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp s5 control]  
user@host# set forwarding-class assured-forwarding
```

- d. Specify a DSCP value in the IP packet header for outbound control packets.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp s5 control]  
user@host# set dscp-code-point 010110
```

**Related  
Documentation**

- [Configuring a Loopback Interface for Transport of GTP Packets on page 304](#)
- [Configuring GTP Services on the S8 Interface on page 310](#)
- [Configuring GTP Services on the Data Plane on page 308](#)
- [Configuring GTP Services on the Control Plane on page 306](#)
- [Configuring GTP Services on a Broadband Gateway on page 305](#)
- [Configuring GTP Services Overview on page 302](#)
- [Configuring General GTP Service on the S-GW on page 325](#)

---

## Configuring GTP Services on the S8 Interface

The following configuration specifies a separate address on which GTP packets (other than Create Session request) are received for a 3GPP S8 interface.

The address you specify for an S8 interface must be the same address specified for the S5 interface although the VRF can be different. In addition, to allow mobility across 3G and LTE, the S8 address must be the same as Gn and Gp addresses, whether or not these addresses are specified explicitly or implicitly (through inheritance or from a higher level).

To configure GTP services on an S8 interface for a broadband gateway configured as a GGSN/P-GW:

1. Configure an IPv4 address on a loopback interface to specify the transport address on which GTP packets are received for the S8 interface.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp s8]
```

```
user@host# set interface lo0.0 v4-address 10.10.10.10
```

2. For tunnel management, configure the maximum number of times that the gateway will attempt to send signaling-request messages to a peer (SGSN or S-GW).

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp s8]
user@host# set n3-requests 6
```

3. For tunnel management, configure the time that the gateway waits before resending a signaling-request message when a response to the request has not been received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp s8]
user@host# set t3-response 8
```

4. For path management, configure the maximum number of times that the gateway will attempt to send an echo-request message to a peer (SGSN or S-GW).

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp s8]
user@host# set echo-n3-requests 6
```

5. For path management, configure the time that the gateway waits before resending an echo-request message when an echo response to the echo request is not received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp s8]
user@host# set echo-t3-response 4
```

6. For path management, configure the number of seconds that the gateway waits before sending an echo-request message after an echo response is received from the peer.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp s8]
user@host# set echo-interval 65
```

7. To configure a separate address on which GTP data packets are received for the S8 interface:

- a. Configure a loopback address.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp s8 data]
user@host# set interface lo0.4 v4-address 10.1.1.8
```



**NOTE:** The path management and tunnel management configuration you specified at the S8 interface level will also apply to GTP data packets unless you configure path management, or tunnel management, or both at the S8 interface data level.

#### Related Documentation

- [Configuring a Loopback Interface for Transport of GTP Packets on page 304](#)
- [Configuring GTP Services on the S5 Interface on page 309](#)
- [Configuring GTP Services on the Data Plane on page 308](#)
- [Configuring GTP Services on the Control Plane on page 306](#)
- [Configuring GTP Services on a Broadband Gateway on page 305](#)
- [Configuring GTP Services Overview on page 302](#)

- [Configuring General GTP Service on the S-GW on page 325](#)

## Configuring GTP Services on the Gn Interface

---

The following configuration specifies the loopback address on which GTP packets are received for a Gn interface.

The IP address you specify for a Gn interface must be the same address that is specified for the Gp interface, although the Gn and Gp interfaces can be in different VRFs. In addition, to support mobility across 3G and 4G networks, the Gn IP address must be the same as the S5 and S8 addresses, optionally, with each interface in a different VRF, whether or not these addresses are specified explicitly or implicitly (through inheritance or from a higher level).

To configure GTP services on a Gn interface for a broadband gateway configured as a GGSN/P-GW:

1. Configure an IPv4 address on a loopback interface to specify the transport address on which GTP packets on the Gn interface are received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp gn]
user@host# set interface lo0.0 v4-address 10.10.10.1
```

2. For tunnel management, configure the maximum number of times that the gateway will attempt to send signaling-request messages to a peer (SGSN or S-GW).

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp gn]
user@host# set n3-requests 6
```

3. For tunnel management, configure the time that the gateway waits before resending a signaling-request message when a response to the request has not been received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp gn]
user@host# set t3-response 8
```

4. For path management, configure the maximum number of times that the gateway will attempt to send an echo-request message to a peer (SGSN or S-GW).

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp gn]
user@host# set echo-n3-requests 6
```

5. For path management, configure the time that the gateway waits before resending an echo-request message when an echo response to the echo request is not received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp gn]
user@host# set echo-t3-response 4
```

6. For path management, configure the number of seconds that the gateway waits before sending an echo-request message after an echo response is received from the peer.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp gn]
```

```
user@host# set echo-interval 65
```

7. To configure a separate loopback address on which GTP control packets are received for the Gn interface:

- a. Configure an IPv4 address on a loopback interface to specify the transport addresses on which GTP control packets on the Gn interface are received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp gn control]
user@host# set interface lo0.5 v4-address 10.10.10.2
```



**NOTE:** The path management and tunnel management configuration you specified at the Gn interface level will also apply to GTP control packets unless you configure path management, or tunnel management, or both at the Gn interface control level.

- b. Specify a forwarding class for outbound control packets.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp gn control]
user@host# set forwarding-class assured-forwarding
```

- c. Specify a DSCP value in the IP packet header for outbound control packets.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp gn control]
user@host# set dscp-code-point 010110
```

#### Related Documentation

- [Configuring a Loopback Interface for Transport of GTP Packets on page 304](#)
- [Configuring GTP Services on the Gp Interface on page 314](#)
- [Configuring GTP Services on the Data Plane on page 308](#)
- [Configuring GTP Services on the Control Plane on page 306](#)
- [Configuring GTP Services on a Broadband Gateway on page 305](#)
- [Configuring GTP Services Overview on page 302](#)
- [Configuring General GTP Service on the S-GW on page 325](#)

## Configuring GTP Services on the Gp Interface

---

The following configuration specifies a separate address on which GTP packets are received for a 3GPP Gp interface.

The IP address you specify for a Gp interface must be the same address that is specified for the Gn interface, although the Gp and Gn interfaces can be in different VRFs. In addition, to allow mobility across 3G and 4G networks, the Gp IP address must be the same as the S5 and S8 addresses (optionally, with each interface in a different VRF) whether or not these addresses are configured explicitly or implicitly (through inheritance or from a higher level).

To configure GTP services on a Gp interface for a broadband gateway configured as a GGSN/P-GW:

1. Configure an IPv4 address on a loopback interface to specify the transport address on which GTP packets on the Gp interface are received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp gp]
user@host# set interface lo0.0 v4-address 10.10.10.1
```

2. For tunnel management, configure the maximum number of times that the gateway will attempt to send signaling-request messages to a peer (SGSN or S-GW).

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp gp]
user@host# set n3-requests 6
```

3. For tunnel management, configure the time that the gateway waits before resending a signaling-request message when a response to the request has not been received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp gp]
user@host# set t3-response 8
```

4. For path management, configure the maximum number of times that the gateway will attempt to send an echo-request message to a peer (SGSN or S-GW).

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp gp]
user@host# set echo-n3-requests 6
```

5. For path management, configure the time that the gateway waits before resending an echo-request message when an echo response to the echo request is not received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp gp]
user@host# set echo-t3-response 4
```

6. For path management, configure the number of seconds that the gateway waits before sending an echo-request message after an echo response is received from the peer.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp gp]
user@host# set echo-interval 65
```

7. To configure a separate loopback address on which GTP control packets are received for the Gp interface:

- a. Configure an IPv4 address on a loopback interface to specify the transport addresses on which GTP control packets on the Gp interface are received.



```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp gp control]
user@host# set interface lo0.5 v4-address 10.10.10.2
```



**NOTE:** The path management and tunnel management configuration you specified at the Gp interface level will also apply to GTP control packets unless you configure path management, or tunnel management, or both at the Gp interface control level.

- b. Specify a forwarding class for outbound control packets.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp gp control]
user@host# set forwarding-class assured-forwarding
```

- c. Specify a DSCP value in the IP packet header for outbound control packets.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp gp control]
user@host# set dscp-code-point 010110
```

#### Related Documentation

- [Configuring a Loopback Interface for Transport of GTP Packets on page 304](#)
- [Configuring GTP Services on the Gn Interface on page 312](#)
- [Configuring GTP Services on the Data Plane on page 308](#)
- [Configuring GTP Services on the Control Plane on page 306](#)
- [Configuring GTP Services on a Broadband Gateway on page 305](#)
- [Configuring GTP Services Overview on page 302](#)
- [Configuring General GTP Service on the S-GW on page 325](#)

## Configuring GTP Services When the S5 and S8 Interfaces Are in Different VRFs

To configure GTP services on a MobileNext Broadband Gateway configured as a P-GW, you specify a different loopback interface but same IP address for each interface when the S5 and S8 interfaces are in different VRF routing instances.

To configure GTP services for a broadband gateway configured as a P-GW when the S5 and S8 interfaces are in different VRFs:

1. Configure the maximum number of peer entries for which the gateway stores statistics collected for deleted peers.

```
[edit unified-edge mobile gateways ggsn-pgw pgw-1 gtp]
user@host# set peer-history 1000
```

2. For tunnel management, configure the maximum number of times that the gateway will attempt to send signaling-request messages to a peer (S-GW).

```
[edit unified-edge mobile gateways ggsn-pgw pgw-1 gtp]
user@host# set n3-requests 6
```

3. For tunnel management, configure the time that the gateway waits before resending a signaling-request message when a response to the request has not been received.

```
[edit unified-edge mobile gateways ggsn-pgw pgw-1 gtp]
user@host# set t3-response 8
```

4. For path management, configure the maximum number of times that the gateway will attempt to send an echo-request message to a peer (SGSN or S-GW).

```
[edit unified-edge mobile gateways ggsn-pgw pgw-1 gtp]
user@host# set echo-n3-requests 6
```

5. For path management, configure the time that the gateway waits before resending an echo-request message when an echo response to the echo request is not received.

```
[edit unified-edge mobile gateways ggsn-pgw pgw-1 gtp]
user@host# set echo-t3-response 4
```

6. For path management, configure the number of seconds that the gateway waits before sending an echo-request message after an echo response is received from the peer.

```
[edit unified-edge mobile gateways ggsn-pgw pgw-1 gtp]
user@host# set echo-interval 65
```

7. Configure a loopback interface and IP address to specify the transport address on which all GTP packets transported on the S5 interface are received.

```
[edit unified-edge mobile gateways ggsn-pgw pgw-1 gtp s5]
user@host# set interface lo0.1 v4-address 10.10.10.10
```



**NOTE:** This interface uses lo0.1.

8. Configure a loopback interface and IP address to specify the transport address on which all GTP packets transported on the S8 interface are received.

```
[edit unified-edge mobile gateways ggsn-pgw pgw-1 gtp s8]
user@host# set interface lo0.2 v4-address 10.10.10.10
```



**NOTE:** This interface uses lo0.2.

9. Configure security trace options for the gateway:
  - a. Specify a name for the file that receives the output of the tracing operation.

```
[edit unified-edge mobile gateways ggsn-pgw pgw-1 gtp traceoptions]
user@host# set file gtp_log
```

- b. Configure the maximum size for the trace file.

```
[edit unified-edge mobile gateways ggsn-pgw pgw-1 gtp traceoptions]
user@host# set size 50m
```

#### Related Documentation

- [Configuring a Loopback Interface for Transport of GTP Packets on page 304](#)
- [Configuring GTP Services on the Data Plane on page 308](#)
- [Configuring GTP Services on the Control Plane on page 306](#)

- [Configuring GTP Services on a Broadband Gateway on page 305](#)
- [Configuring GTP Services Overview on page 302](#)
- [Configuring General GTP Service on the S-GW on page 325](#)

## Configuring GTP Services When the S5 and S8 Interfaces Are in the Same VRF

When the interfaces are in the same VRF routing instances, you specify a single loopback interface IP address for the S5 and S8 interfaces.

To configure GTP services for a MobileNext Broadband Gateway configured as a P-GW when the S5 and S8 interfaces are in the same VRF:

1. Configure the maximum number of peer entries for which the gateway stores statistics collected for deleted peers.

```
[edit unified-edge mobile gateways ggsn-pgw pgw-vrf-green gtp]
user@host# set peer-history 1000
```

2. For tunnel management, configure the maximum number of times that the gateway will attempt to send signaling-request messages to a peer (SGSN or S-GW).

```
[edit unified-edge mobile gateways ggsn-pgw pgw-vrf-green gtp]
user@host# set n3-requests 6
```

3. For tunnel management, configure the time that the gateway waits before resending a signaling-request message when a response to the request has not been received.

```
[edit unified-edge mobile gateways ggsn-pgw pgw-vrf-green gtp]
user@host# set t3-response 8
```

4. For path management, configure the maximum number of times that the gateway will attempt to send an echo-request message to a peer (SGSN or S-GW).

```
[edit unified-edge mobile gateways ggsn-pgw pgw-vrf-green gtp]
user@host# set echo-n3-requests 6
```

5. For path management, configure the time that the gateway waits before resending an echo-request message when an echo response to the echo request is not received.

```
[edit unified-edge mobile gateways ggsn-pgw pgw-vrf-green gtp]
user@host# set echo-t3-response 4
```

6. For path management, configure the number of seconds that the gateway waits before sending an echo-request message after an echo response is received from the peer.

```
[edit unified-edge mobile gateways ggsn-pgw pgw-vrf-green gtp]
user@host# set echo-interval 65
```

7. Configure a loopback interface and IP address to specify the transport address on which all GTP packets transported on the S5 interface are received

```
[edit unified-edge mobile gateways ggsn-pgw pgw-vrf-green gtp s5]
user@host# set interface lo0.1 v4-address 10.10.10.10
```



**NOTE:** This interface uses lo0.1.

8. Configure a loopback interface and IP address to specify the transport address on which all GTP packets transported on the S8 interface are received

```
[edit unified-edge mobile gateways ggsn-pgw pgw-vrf-green gtp s8]
user@host# set interface lo0.1 v4-address 10.10.10.10
```



**NOTE:** This interface also uses lo0.1.

9. Configure security trace options for the gateway:

- a. Specify a name for the file that receives the output of the tracing operation.

```
[edit unified-edge mobile gateways ggsn-pgw pgw-vrf-green gtp traceoptions]
user@host# set file gtp_log
```

- b. Configure the maximum size for the trace file.

```
[edit unified-edge mobile gateways ggsn-pgw pgw-vrf-green gtp traceoptions]
user@host# set size 50m
```

#### Related Documentation

- [Configuring a Loopback Interface for Transport of GTP Packets on page 304](#)
- [Configuring GTP Services on the Data Plane on page 308](#)
- [Configuring GTP Services on the Control Plane on page 306](#)
- [Configuring GTP Services on a Broadband Gateway on page 305](#)
- [Configuring GTP Services Overview on page 302](#)
- [Configuring General GTP Service on the S-GW on page 325](#)

## Configuring GTP Services When 3GPP Interfaces Are in Different VRFs

To configure GTP services on a MobileNext Broadband Gateway when the Gn , Gp, S5, and S8 interfaces are in different VRFs, you configure each interface with a different loopback interface but must specify the same IP address for the Gn , Gp, S5, and S8 interfaces.

In this example configuration, the same GTP services configuration is applied across the Gn, Gp, S5, and S8 interfaces. However, for each interface, GTP packets will be received on a separate loopback interface but specifying the same IP address.

To configure GTP services for a broadband gateway configured as a GGSN/P-GW on which the interfaces use different VRFs:

1. Configure the maximum number of peer entries for which the gateway stores statistics collected for deleted peers.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp]
```

```
user@host# set peer-history 1000
```

2. For tunnel management, configure the maximum number of times that the gateway will attempt to send signaling-request messages to a peer (SGSN or S-GW).

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp]
user@host# set n3-requests 6
```

3. For tunnel management, configure the time that the gateway waits before resending a signaling-request message when a response to the request has not been received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp]
user@host# set t3-response 8
```

4. For path management, configure the maximum number of times that the gateway will attempt to send an echo-request message to a peer (SGSN or S-GW).

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp]
user@host# set echo-n3-requests 6
```

5. For path management, configure the time that the gateway waits before resending an echo-request message when an echo response to the echo request is not received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp]
user@host# set echo-t3-response 4
```

6. For path management, configure the number of seconds that the gateway waits before sending an echo-request message after an echo response is received from the peer.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp]
user@host# set echo-interval 65
```

7. Configure a loopback interface and IP address to specify the transport address on which all GTP packets transported on the S5 interface are received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp s5]
user@host# set interface lo0.1 v4-address 10.10.10.10
```

8. Configure a loopback interface and IP address to specify the transport address on which all GTP packets transported on the S8 interface are received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp s8]
user@host# set interface lo0.2 v4-address 10.10.10.10
```

9. Configure a loopback interface and IP address to specify the transport address on which all GTP packets transported on the Gn interface are received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp gn]
user@host# set interface lo0.3 v4-address 10.10.10.10
```

10. Configure a loopback interface and IP address to specify the transport address on which all GTP packets transported on the Gp interface are received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp gp]
user@host# set interface lo0.4 v4-address 10.10.10.10
```

11. Configure security trace options for the gateway:

- a. Specify a name for the file that receives the output of the tracing operation.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp traceoptions]
```

```
user@host# set file gtp_log
```

- b. Configure the maximum size for the trace file.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp traceoptions]  
user@host# set size 50m
```

**Related  
Documentation**

- [Configuring a Loopback Interface for Transport of GTP Packets on page 304](#)
- [Configuring GTP Services on the Data Plane on page 308](#)
- [Configuring GTP Services on the Control Plane on page 306](#)
- [Configuring GTP Services on a Broadband Gateway on page 305](#)
- [Configuring GTP Services Overview on page 302](#)
- [Configuring General GTP Service on the S-GW on page 325](#)

---

## Configuring GTP Services on a GGSN Broadband Gateway

When you configure GTP services on a MobileNext Broadband Gateway configured as a GGSN, you can optionally specify a different address on which GTP control or data packets are received for the Gn and Gp interfaces.

In this example 3G configuration, the Gn and Gp interfaces are in the same VRF routing instance. The Gn interface configuration specifies that GTP-C and GTP-U packets (on the Gn interface) are each received on a different transport address. The Gp interface configuration specifies that all GTP packets (on the Gp interface) are received on a single transport address.

To configure GTP services for a broadband gateway configured as a GGSN:

1. Configure the maximum number of peer entries for which the gateway stores statistics collected for deleted peers.

```
[edit unified-edge mobile gateways ggsn-pgw ggsn-1 gtp]  
user@host# set peer-history 1000
```

2. For tunnel management, configure the maximum number of times that the gateway will attempt to send signaling-request messages to a peer (SGSN or S-GW).

```
[edit unified-edge mobile gateways ggsn-pgw ggsn-1 gtp]  
user@host# set n3-requests 6
```

3. For tunnel management, configure the time that the gateway waits before resending a signaling-request message when a response to the request has not been received.

```
[edit unified-edge mobile gateways ggsn-pgw ggsn-1 gtp]  
user@host# set t3-response 8
```

4. For path management, configure the maximum number of times that the gateway will attempt to send an echo-request message to a peer (SGSN or S-GW).

```
[edit unified-edge mobile gateways ggsn-pgw ggsn-1 gtp]  
user@host# set echo-n3-requests 6
```

5. For path management, configure the time that the gateway waits before resending an echo-request message when an echo response to the echo request is not received.

```
[edit unified-edge mobile gateways ggsn-pgw ggsn-1 gtp]
user@host# set echo-t3-response 4
```

6. For path management, configure the number of seconds that the gateway waits before sending an echo-request message after an echo response is received from the peer.

```
[edit unified-edge mobile gateways ggsn-pgw ggsn-1 gtp]
user@host# set echo-interval 65
```

7. Configure a loopback address to specify the transport address on which GTP packets transported on the Gn interface are received.

```
[edit unified-edge mobile gateways ggsn-pgw ggsn-1 gtp gn]
user@host# set interface lo0.1 v4-address 10.10.10.10
```

8. Configure a loopback address to specify a different transport address on which GTP data packets transported on the Gn interface are received.

```
[edit unified-edge mobile gateways ggsn-pgw ggsn-1 gtp gn data]
user@host# set interface lo0.1 v4-address 10.10.10.20
```

9. Configure a loopback interface and IP address to specify the transport address on which all GTP packets transported on the Gp interface are received.

```
[edit unified-edge mobile gateways ggsn-pgw ggsn-1 gtp gp]
user@host# set interface lo0.1 v4-address 10.10.10.30
```

**Related  
Documentation**

- [Configuring a Loopback Interface for Transport of GTP Packets on page 304](#)
- [Configuring GTP Services Overview on page 302](#)
- [Configuring GTP Services on the Data Plane on page 308](#)
- [Configuring GTP Services on the Control Plane on page 306](#)
- [Configuring GTP Services on a Broadband Gateway on page 305](#)
- [Configuring GTP Services When 3GPP Interfaces Are in Different VRFs on page 318](#)
- [Configuring General GTP Service on the S-GW on page 325](#)

---

## Configuring GTP Services on a Peer Group

You can configure GTP services to overwrite default configurations for a group of SGSN or S-GW peers.

To configure GTP services on a peer group:

1. Specify a name for the peer group.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp]
user@host# edit peer-groups peer-grp-1
```

2. Specify the name of the routing instance to which all peers in the peer group belong.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp peer-groups peer-grp-1]
user@host# set routing-instance vrf-instance-peers-green
```

3. Configure the IP addresses for the peers in the peer group.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp peer-groups peer-grp-1]
user@host# set peer 22.1.1.10/16
```

4. For tunnel management, configure the maximum number of times that the gateway will attempt to send signaling-request messages to a peer (SGSN or S-GW).

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp peer-groups peer-grp-1]
user@host# set n3-requests 6
```

5. For tunnel management, configure the time that the gateway waits before resending a signaling-request message when a response to the request has not been received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp peer-groups peer-grp-1]
user@host# set t3-response 8
```

6. For path management, configure the maximum number of times that the gateway will attempt to send an echo-request message to a peer (SGSN or S-GW).

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp peer-groups peer-grp-1]
user@host# set echo-n3-requests 6
```

7. For path management, configure the time that the gateway waits before resending an echo-request message when an echo response to the echo request is not received.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp peer-groups peer-grp-1]
user@host# set echo-t3-response 4
```

8. For path management, configure the number of seconds that the gateway waits before sending an echo-request message after an echo response is received from the peer.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp peer-groups peer-grp-1]
user@host# set echo-interval 65
```

9. Configure the peer gateways to transport a 16-bit sequence number when GTP control packets are sent to and received from the peer gateways.

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp peer-groups peer-grp-1 control]
user@host# set sequence-number-length 16-bits
```

**Related  
Documentation**

- [Configuring a Loopback Interface for Transport of GTP Packets on page 304](#)
- [Configuring GTP Services on the Data Plane on page 308](#)
- [Configuring GTP Services on the Control Plane on page 306](#)
- [Configuring GTP Services on a Broadband Gateway on page 305](#)
- [Configuring GTP Services Overview on page 302](#)
- [Configuring General GTP Service on the S-GW on page 325](#)



## Disabling Path Management on a Broadband Gateway or Peer Group

You can temporarily disable path management on the MobileNext Broadband Gateway so that echo-request messages are not sent from the P-GW to a peer.

When you configure the broadband gateway as a P-GW, the path management options are automatically enabled using the default echo-timing values. You can configure the **path-management** option to temporarily disable path management on the entire gateway, or on the control plane, data plane, or interface (S5, S8, Gn, or Gp) level.

- To disable path management on the Broadband Gateway:

```
[edit unified-edge mobile gateways ggsn-pdn-gateway MBG1 gtp
user@host# set path-management disable
```

To enable echo-request processing again on the GGSN/P-GW:

```
[edit unified-edge mobile gateways ggsn-pdn-gateway MBG1 gtp
user@host# set path-management enable
```

- To disable path management on a peer group:

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp peer-groups peer-grp-1]
user@host# set path-management disable
```

To enable path management again on the peer group:

```
[edit unified-edge mobile gateways ggsn-pgw MBG1 gtp peer-groups peer-grp-1]
user@host# set path-management enable
```

### Related Documentation

- [GTP Path Management Overview on page 290](#)
- [Configuring GTP Services Overview on page 302](#)
- [Configuring General GTP Service on the S-GW on page 325](#)

## Configuring GTP Trace Options

GTP tracing operations record detailed messages about the operation of GTP services on the Broadband Gateway, such as the various types of GTP packets sent and received, GTP peer-related events, GTP tracker-related events, configuration information, and debug information. You can specify which trace operations are logged by including specific tracing flags and levels.

[Table 42 on page 323](#) describes the flags that you can include.

Table 42: Trace Flags

| Flag          | Description                              |
|---------------|------------------------------------------|
| <b>all</b>    | Trace everything.                        |
| <b>config</b> | Trace configuration-related information. |
| <b>debug</b>  | Trace debug information.                 |

Table 42: Trace Flags (*continued*)

|                  |                                         |
|------------------|-----------------------------------------|
| <b>decode</b>    | Trace decoding of received packets.     |
| <b>encode</b>    | Trace encoding of transmitted packets.  |
| <b>events</b>    | Trace all internal and external events. |
| <b>packet-io</b> | Trace transmitted and received packets. |
| <b>peer</b>      | Trace decoding of received packets.     |
| <b>tracker</b>   | Trace GTP peer-related events.          |
| <b>warning</b>   | Trace warnings.                         |

[Table 43 on page 324](#) describes the levels you can include.

Table 43: Trace Levels

| Level          | Description                                        |
|----------------|----------------------------------------------------|
| <b>all</b>     | Match all levels.                                  |
| <b>error</b>   | Match error conditions.                            |
| <b>info</b>    | Match informational messages.                      |
| <b>notice</b>  | Match conditions that should be specially handled. |
| <b>verbose</b> | Match verbose messages.                            |
| <b>warning</b> | Match warning messages.                            |

To configure tracing options for GTP operations:

- Specify that you want to configure tracing options for GTP operations.  

```
[edit unified-edge gateways ggsn-pgw pgw-1 gtp]
user@host# edit traceoptions
```
- Configure the filename for the trace file.  

```
[edit unified-edge mobile gateways ggsn-pgw pgw-1 gtp trace-options]
user@host# set file gtp-log
```
- (Optional) Configure the maximum size of each trace file.  

```
[edit unified-edge mobile gateways ggsn-pgw pgw-1 gtp trace-options]
user@host# set file size 100m
```
- Configure tracing flags.  

```
[edit unified-edge mobile gateways ggsn-pgw pgw-1 gtp s5 trace-options]
user@host# set flag all
```

5. Configure the tracing level.

```
[edit unified-edge mobile gateways ggsn-pgw pgw-1 gtp s5 trace-options]
user@host# set level error
```

6. View the trace file.

```
user@host# file show /var/log/gtp-log
```

**Related  
Documentation**

- [Configuring GTP Services Overview on page 302](#)
- [Configuring General GTP Service on the S-GW on page 325](#)

## Configuring General GTP Service on the S-GW

The following configuration specifies the general parameters for the GPRS Tunneling Protocol (GTP) for a Serving Gateway (S-GW) configured on the MobileNext Broadband Gateway. GTP includes control (GTP-C) version 2 and GTP, user (GTP-U) payloads inside UDP datagrams. Parameters configured at the more specific hierarchy level override those configured at a more general hierarchy level.

You can configure many of the same parameters for GTP-C (**control**) and GTP-U (**data**) payloads as at the GTP (**gtp**) hierarchy level. When configured as separate control or data parameters, these values override the values configured at the **gtp** hierarchy level.

You can configure the following parameters at multiple GTP hierarchy levels:

- **echo-interval**
- **echo-n3-requests**
- **echo-t3-response**
- **interface**
- **n3-requests** (except data level)
- **path-management**
- **t3-response** (except data level)

To configure GTP services for a broadband gateway configured as an S-GW called MBG2:

1. Configure the maximum number of GTP peers for which statistics are stored in the GTP history.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
user@host# set peer-history 100
```



**NOTE:** You can set the peers for which statistics are stored from 1 to 1000. There is no default value.

2. Configure an interface to use for GTP packets. If the interface has more than one IP address, specify which address to use.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp control]
[edit unified-edge mobile gateways sgw MBG2 gtp data]
user@host# set interface lo0.2 v4-address 10.10.10.2
```

3. (Optional) Disable or enable path management.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp control]
[edit unified-edge mobile gateways sgw MBG2 gtp data]
user@host# set path-management disable
```



**NOTE:** Control path management is enabled by default for the GTP control plane (GTP-C), but disabled by default for the GTP user plane (GTP-U).

4. For tunnel management, configure the maximum number of times that the gateway will attempt to send signaling-request messages to a remote control peer.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp control]
user@host# set n3-requests 6
```



**NOTE:** This parameter cannot be set for data (GTP-U).

5. For tunnel management, configure the time that the gateway waits before resending a signaling-request message when a response to the request has not been received.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp control]
user@host# set t3-response 8
```



**NOTE:** This parameter cannot be set for data (GTP-U).

6. For path management, configure the maximum number of times that the gateway will attempt to send an echo-request message to a remote control peer.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp control]
[edit unified-edge mobile gateways sgw MBG2 gtp data]
user@host# set echo-n3-requests 6
```

7. For path management, configure the time that the gateway waits before resending an echo-request message when an echo response to the echo request is not received.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp control]
[edit unified-edge mobile gateways sgw MBG2 gtp data]
user@host# set echo-t3-response 4
```

8. For path management, configure the number of seconds that the gateway waits before sending an echo-request message after an echo response is received from the peer.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp control]
[edit unified-edge mobile gateways sgw MBG2 gtp data]
user@host# set echo-interval 65
```

9. To configure parameters for GTP-U data packets:

a. Specify the error indication interval.

```
[edit unified-edge mobile gateways sgw MBG2 gtp data]
user@host# set error-indication-interval 5
```



**NOTE:** You can set the error indication interval from 1 to 20 seconds. The default value is 1 second.

b. (Optional) Enable the indirect tunnel feature.

```
[edit unified-edge mobile gateways sgw MBG2 gtp data]
user@host# set indirect-tunnel
```



**NOTE:** The indirect tunnel feature is enabled by default.

10. To configure parameters for GTP-C control packets:

a. (Optional) Disable the GTP response cache.

```
[edit unified-edge mobile gateways sgw MBG2 gtp control]
user@host# set no-response-cache
```



**NOTE:** The GTP response cache is enabled by default.

b. (Optional) Specify a response cache timeout value for cached GTP response packets.

```
[edit unified-edge mobile gateways sgw MBG2 gtp control]
user@host# set response-cache-timeout 10
```



**NOTE:** You can set the response cache timer from 5 to 20 seconds.

c. Specify a forwarding class for outbound control packets.

```
[edit unified-edge mobile gateways sgw MBG2 gtp control]
user@host# set forwarding-class assured-forwarding
```

d. Specify a DSCP value in the IP packet header for outbound control packets.

```
[edit unified-edge mobile gateways sgw MBG2 gtp control]
user@host# set dscp-code-point 010110
```

e. Enable or disable the downlink data notification delay synchronization across service PICs.

```
[edit unified-edge mobile gateways sgw MBG2 gtp control]
user@host# set ddn-delay-sync
```



**NOTE:** By default, downlink data notification delay synchronization is enabled.

- f. Specify a time-to-live (TTL) value to be used in the GTP-C packets.

```
[edit unified-edge mobile gateways sgw MBG2 gtp control]
user@host# set ttl-value 1
```



**NOTE:** By default, the TTL value is 255. You can set any value from 1 to 255.

#### Related Documentation

- [GPRS Tunneling Protocol \(GTP\) Overview on page 289](#)
- [Configuring GTP Services on the S4 Interface on page 333](#)
- [Configuring GTP-C Services on the S11 Interface on page 328](#)
- [Configuring GTP-U Services on the S12 Interface on page 330](#)
- [Configuring GTP Services on the S1-U Interface on page 332](#)
- [Example: Configuring GTP for the S-GW When Interfaces Are in different VRFs on page 340](#)

---

## Configuring GTP-C Services on the S11 Interface

The following configuration specifies the parameters for a 3GPP S11 interface on the MobileNext Broadband Gateway. The S11 interface is between the Serving Gateway (S-GW) and the Mobility Management Entity (MME). The S11 interface processes GPRS tunneling protocol, control (GTP-C) version 2 payloads inside UDP datagrams.

You can configure many of the same parameters for the GTP (**gtp**) hierarchy level and the S11 (**s11**) interface hierarchy level. When configured as separate GTP or interface parameters, the values at the S11 (**s11**) hierarchy level override the values configured at the GTP (**gtp**) hierarchy level.

You can configure the following parameters at the GTP and S11 hierarchy levels:

- **echo-interval**
- **echo-n3-requests**
- **echo-t3-response**
- **interface**
- **n3-requests**

- path-management
- t3-response

To configure GTP-Cv2 services on an S11 interface for a broadband gateway configured as a S-GW named MBG2:

1. Configure an IPv4 address on a loopback interface to specify the transport addresses on which GTP-Cv2 packets on the S11 interface are received.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp s11]
user@host# set interface lo0.2 v4-address 10.10.10.1
```

2. Specify a DSCP value in the IP packet header for outbound control packets.

```
[edit unified-edge mobile gateways sgw MBG2 gtp s11]
user@host# set dscp-code-point 010110
```

3. Specify a time-to-live (TTL) value to be used in the GTP-C packets.

```
[edit unified-edge mobile gateways sgw MBG2 gtp s11]
user@host# set ttl-value 1
```



**NOTE:** By default, the TTL value is 255. You can set any value from 1 to 255.

4. Optionally, disable or enable path management.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp s11]
user@host# set path-management disable
```



**NOTE:** Path management is enabled by default.

5. For tunnel management, configure the maximum number of times that the gateway will attempt to send signaling-request messages to an MME.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp s11]
user@host# set n3-requests 6
```

6. For tunnel management, configure the time that the gateway waits before resending a signaling-request message when a response to the request has not been received.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp s11]
user@host# set t3-response 8
```

7. For path management, configure the maximum number of times that the gateway will attempt to send an echo-request message to an MME.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp s11]
user@host# set echo-n3-requests 6
```

8. For path management, configure the time that the gateway waits before resending an echo-request message when an echo response to the echo request is not received.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp s11]
user@host# set echo-t3-response 4
```

9. For path management, configure the number of seconds that the gateway waits before sending an echo-request message after an echo response is received from the MME.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp s11]
user@host# set echo-interval 65
```

**Related  
Documentation**

- [GPRS Tunneling Protocol \(GTP\) Overview on page 289](#)
- [Configuring General GTP Service on the S-GW on page 325](#)
- [Configuring GTP Services on the S4 Interface on page 333](#)
- [Configuring GTP-U Services on the S12 Interface on page 330](#)
- [Configuring GTP Services on the S1-U Interface on page 332](#)
- [Example: Configuring GTP for the S-GW When Interfaces Are in different VRFs on page 340](#)

---

## Configuring GTP-U Services on the S12 Interface

The following configuration specifies the parameters for a 3GPP S12 interface on the MobileNext Broadband Gateway. The S12 interface is between the Serving Gateway (S-GW) and a 3G mobile radio network, specifically, the Radio Network Controller (RNC). The S12 interface processes GPRS tunneling protocol, user (GTP-U) payloads inside UDP datagrams.

You can configure many of the same parameters for the GTP (**gtp**) hierarchy level and the S12 (**s12**) interface hierarchy level. When configured as separate GTP or interface parameters, the values at the S12 (**s12**) hierarchy level override the values configured at the GTP (**gtp**) hierarchy level.

You can configure the following parameters at the GTP and S12 hierarchy levels:

- **echo-interval**
- **echo-n3-requests**
- **echo-t3-response**
- **interface**
- **path-management**



To configure GTP-U services on an S12 interface for a broadband gateway configured as an S-GW named MBG2:

1. Configure an IPv4 address on a loopback interface to specify the transport addresses on which GTP-U packets on the S12 interface are received.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp s12]
user@host# set interface lo0.2 v4-address 10.10.10.2
```

2. (Optional) Enable path management.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp s12]
user@host# set path-management enable
```



**NOTE:** Path management on the S12 interface is disabled by default.

3. For path management, configure the maximum number of times that the gateway will attempt to send an echo-request message to an RNC.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp s12]
user@host# set echo-n3-requests 6
```

4. For path management, configure the time that the gateway waits before resending an echo-request message when an echo response to the echo request is not received.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp s12]
user@host# set echo-t3-response 4
```

5. For path management, configure the number of seconds that the gateway waits before sending an echo-request message after an echo response is received.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp s12]
user@host# set echo-interval 65
```

#### Related Documentation

- [GPRS Tunneling Protocol \(GTP\) Overview on page 289](#)
- [Configuring General GTP Service on the S-GW on page 325](#)
- [Configuring GTP Services on the S4 Interface on page 333](#)
- [Configuring GTP-C Services on the S11 Interface on page 328](#)
- [Configuring GTP Services on the S1-U Interface on page 332](#)
- [Example: Configuring GTP for the S-GW When Interfaces Are in different VRFs on page 340](#)

## Configuring GTP Services on the S1-U Interface

---

The following configuration specifies the parameters for a 3GPP S1-U interface on the MobileNext Broadband Gateway. The S1-U interface is between the Serving Gateway (S-GW) and a mobile radio network, specifically, the enhanced Node B (eNodeB). The S1-U interface processes GPRS tunneling protocol, user (GTP-U) payloads inside UDP datagrams.

You can configure many of the same parameters for the GTP (**gtp**) hierarchy level and the S1-U (**s1u**) interface hierarchy level. When configured as separate GTP or interface parameters, the values at the S1-U (**s1u**) hierarchy level override the values configured at the GTP (**gtp**) hierarchy level.

You can configure the following parameters at the GTP and S1-U hierarchy levels:

- **echo-interval**
- **echo-n3-requests**
- **echo-t3-response**
- **interface**
- **path-management**

To configure GTP-U services on an S1-U interface for a broadband gateway configured as an S-GW named MBG2:

1. Configure an IPv4 or IPv6 address on a loopback interface to specify the transport addresses on which GTP-U packets on the S1-U interface are received.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp s1u]
user@host# set interface lo0.2 v4-address 10.10.10.2
```

2. (Optional) Enable path management.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp s1u]
user@host# set path-management enable
```



**NOTE:** Path management on the S1-U interface is disabled by default.

---

3. For path management, configure the maximum number of times that the gateway will attempt to send an echo-request message to an eNodeB.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp s1u]
user@host# set echo-n3-requests 6
```

4. For path management, configure the time that the gateway waits before resending an echo-request message when an echo response to the echo request is not received.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp s1u]
```

```
user@host# set echo-t3-response 4
```

- For path management, configure the number of seconds that the gateway waits before sending an echo-request message after an echo response is received.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp s1u]
user@host# set echo-interval 65
```

#### Related Documentation

- [GPRS Tunneling Protocol \(GTP\) Overview on page 289](#)
- [Configuring General GTP Service on the S-GW on page 325](#)
- [Configuring GTP Services on the S4 Interface on page 333](#)
- [Configuring GTP-C Services on the S11 Interface on page 328](#)
- [Configuring GTP-U Services on the S12 Interface on page 330](#)
- [Example: Configuring GTP for the S-GW When Interfaces Are in different VRFs on page 340](#)

## Configuring GTP Services on the S4 Interface

The following configuration specifies the parameters for a 3GPP S4 interface on the MobileNext Broadband Gateway. The S4 interface is between the Serving Gateway (S-GW) and a Serving GPRS Support Node (SGSN). The S4 interface processes GPRS tunneling protocol, control (GTP-C) version 2 and GTP, user (GTP-U) payloads inside UDP datagrams.

You can configure many of the same parameters for GTP-C (control) and GTP-U (data) payloads on the S4 interface. When configured as separate interface, control, or data parameters, these values override the values configured at the GTP (**gtp**) hierarchy level. Parameters at the control or data level override those set at the S4 (**s4**) hierarchy level.

You can configure the following parameters at multiple GTP hierarchy levels:

- **echo-interval**
- **echo-n3-requests**
- **echo-t3-response**
- **interface**
- **n3-requests** (all levels except S4 data)
- **path-management**
- **t3-response** (all levels except S4 data)

To configure GTP services on an S4 interface for a broadband gateway configured as an S-GW called MBG2:

- Configure an interface to use for GTP packets. If the interface has more than one IP address, you can specify which address to use.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp s4]
[edit unified-edge mobile gateways sgw MBG2 gtp s4 control]
[edit unified-edge mobile gateways sgw MBG2 gtp s4 data]
user@host# set interface lo0.2 v4-address 10.10.10.2
```

2. (Optional) Disable or enable path management.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp s4]
[edit unified-edge mobile gateways sgw MBG2 gtp s4 control]
[edit unified-edge mobile gateways sgw MBG2 gtp s4 data]
user@host# set path-management disable
```



**NOTE:** Path management is enabled by default.

3. For tunnel management, configure the maximum number of times that the gateway will attempt to send signaling-request messages to an SGSN.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp s4]
[edit unified-edge mobile gateways sgw MBG2 gtp s4 control]
user@host# set n3-requests 6
```



**NOTE:** This parameter cannot be set for S4 data (GTP-U).

4. For tunnel management, configure the time that the gateway waits before resending a signaling-request message when a response to the request has not been received.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp s4]
[edit unified-edge mobile gateways sgw MBG2 gtp s4 control]
user@host# set t3-response 8
```



**NOTE:** This parameter cannot be set for S4 data (GTP-U).

5. For path management, configure the maximum number of times that the gateway will attempt to send an echo-request message to an SGSN.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp s4]
[edit unified-edge mobile gateways sgw MBG2 gtp s4 control]
[edit unified-edge mobile gateways sgw MBG2 gtp s4 data]
user@host# set echo-n3-requests 6
```

6. For path management, configure the time that the gateway waits before resending an echo-request message when an echo response to the echo request is not received.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp s4]
[edit unified-edge mobile gateways sgw MBG2 gtp s4 control]
[edit unified-edge mobile gateways sgw MBG2 gtp s4 data]
user@host# set echo-t3-response 4
```

7. For path management, configure the number of seconds that the gateway waits before sending an echo-request message after an echo response is received from the peer.

```
[edit unified-edge mobile gateways sgw MBG2 gtp]
[edit unified-edge mobile gateways sgw MBG2 gtp s4]
[edit unified-edge mobile gateways sgw MBG2 gtp s4 control]
[edit unified-edge mobile gateways sgw MBG2 gtp s4 data]
user@host# set echo-interval 65
```

8. To configure parameters for GTP control packets for the S4 interface:

- a. Specify a forwarding class for outbound control packets.

```
[edit unified-edge mobile gateways sgw MBG2 gtp s4 control]
user@host# set forwarding-class assured-forwarding
```

- b. Specify a DSCP value in the IP packet header for outbound control packets.

```
[edit unified-edge mobile gateways sgw MBG2 gtp s4 control]
user@host# set dscp-code-point 010110
```

#### Related Documentation

- [GPRS Tunneling Protocol \(GTP\) Overview on page 289](#)
- [Configuring General GTP Service on the S-GW on page 325](#)
- [Configuring GTP-C Services on the S11 Interface on page 328](#)
- [Configuring GTP-U Services on the S12 Interface on page 330](#)
- [Example: Configuring GTP for the S-GW When Interfaces Are in different VRFs on page 340](#)

## Configuring GTP Services on the S-GW When the S4 and S5 Interfaces Are in the Same VRF

To configure GTP services on a MobileNext Broadband Gateway configured as a Service Gateway (S-GW) when the S4 (between Serving GPRS Support Node [SGSN] and S-GW) and S5 (between S-GW and Packet Data Network Gateway [P-GW]) interfaces are the same virtual routing and forwarding (VRF) routing instances, you specify a single loopback interface IP address for the S4 and S5 interfaces.

To configure GTP services for a MobileNext Broadband Gateway configured as a S-GW when the S4 and S5 interfaces are in the same VRF:

1. Configure the maximum number of peer entries for which the gateway stores statistics collected for deleted peers.

```
[edit unified-edge mobile gateways sgw SGW--vrf-green gtp]
user@host# set peer-history 1000
```

2. For tunnel management, configure the maximum number of times that the gateway will attempt to send signaling-request messages to a peer.

```
[edit unified-edge mobile gateways sgw SGW--vrf-green gtp]
user@host# set n3-requests 6
```

3. For tunnel management, configure the time that the gateway waits before resending a signaling-request message when a response to the request has not been received.

```
[edit unified-edge mobile gateways sgw SGW--vrf-green gtp]
user@host# set t3-response 8
```

4. For path management, configure the maximum number of times that the gateway will attempt to send an echo-request message to a peer.

```
[edit unified-edge mobile gateways sgw SGW--vrf-green gtp]
user@host# set echo-n3-requests 6
```

5. For path management, configure the time that the gateway waits before resending an echo-request message when an echo response to the echo request is not received.

```
[edit unified-edge mobile gateways sgw SGW--vrf-green gtp]
user@host# set echo-t3-response 4
```

6. For path management, configure the number of seconds that the gateway waits before sending an echo-request message after an echo response is received from the peer.

```
[edit unified-edge mobile gateways sgw SGW--vrf-green gtp]
user@host# set echo-interval 65
```

7. Configure a loopback interface and IP address to specify the transport address on which all GTP packets transported on the S4 interface are received

```
[edit unified-edge mobile gateways sgw SGW--vrf-green gtp s4]
user@host# set interface lo0.1 v4-address 10.10.10.10
```



**NOTE:** This interface uses lo0.1.

8. Configure a loopback interface and IP address to specify the transport address on which all GTP packets transported on the S5 interface are received

```
[edit unified-edge mobile gateways sgw SGW--vrf-green gtp s5]
user@host# set interface lo0.1 v4-address 10.10.10.10
```



**NOTE:** This interface also uses lo0.1.

9. Configure security trace options for the gateway:

- a. Specify a name for the file that receives the output of the tracing operation.

```
[edit unified-edge mobile gateways sgw SGW-vrf-green gtp traceoptions]
user@host# set file gtp_log
```

- b. Configure the maximum size for the trace file.

```
[edit unified-edge mobile gateways spgw SGW-vrf-green gtp traceoptions]
user@host# set size 50m
```

**Related  
Documentation**

- [Configuring General GTP Service on the S-GW on page 325](#)
- [Configuring GTP Services on the S4 Interface on page 333](#)

- [Configuring GTP Services on the S5 Interface on page 309](#)
- [GPRS Tunneling Protocol \(GTP\) Overview on page 289](#)

## Configuring GTP Services on the S-GW When Interfaces are in Different VRFs

To configure GTP services on a MobileNext Broadband Gateway configured as a S-GW when the S4 (between Serving GPRS Support Node [SGSN] and S-GW) and S5 (between S-GW and Packet Data Network Gateway [P-GW]) interfaces are in different virtual routing and forwarding (VRF) routing instances, you specify a different loopback interface but same IP address for each interface.

To configure GTP services for a broadband gateway configured as a S-GW when the S4 and S5 interfaces are in different VRFs:

1. Configure the maximum number of peer entries for which the gateway stores statistics collected for deleted peers.

```
[edit unified-edge mobile gateways sgw SGW-1 gtp]
user@host# set peer-history 1000
```

2. For tunnel management, configure the maximum number of times that the gateway will attempt to send signaling-request messages to a peer.

```
[edit unified-edge mobile gateways sgw SGW-1 gtp]
user@host# set n3-requests 6
```

3. For tunnel management, configure the time that the gateway waits before resending a signaling-request message when a response to the request has not been received.

```
[edit unified-edge mobile gateways sgw SGW-1 gtp]
user@host# set t3-response 8
```

4. For path management, configure the maximum number of times that the gateway will attempt to send an echo-request message to a peer (SGSN or S-GW).

```
[edit unified-edge mobile gateways sgw SGW-1 gtp]
user@host# set echo-n3-requests 6
```

5. For path management, configure the time that the gateway waits before resending an echo-request message when an echo response to the echo request is not received.

```
[edit unified-edge mobile gateways sgw SGW-1 gtp]
user@host# set echo-t3-response 4
```

6. For path management, configure the number of seconds that the gateway waits before sending an echo-request message after an echo response is received from the peer.

```
[edit unified-edge mobile gateways sgw SGW-1 gtp]
user@host# set echo-interval 65
```

7. Configure a loopback interface and IP address to specify the transport address on which all GTP packets transported on the S4 interface are received.

```
[edit unified-edge mobile gateways sgw SGW-1 gtp s4]
user@host# set interface lo0.1 v4-address 10.10.10.10
```



**NOTE:** This interface uses lo0.1.

8. Configure a loopback interface and IP address to specify the transport address on which all GTP packets transported on the S5 interface are received.

```
[edit unified-edge mobile gateways sgw SGW-1 gtp s5]
user@host# set interface lo0.2 v4-address 10.10.10.10
```



**NOTE:** This interface uses lo0.2.

9. Configure security trace options for the gateway:
  - a. Specify a name for the file that receives the output of the tracing operation.

```
[edit unified-edge mobile gateways sgw SGW-1 gtp traceoptions]
user@host# set file gtp_log
```

- b. Configure the maximum size for the trace file.

```
[edit unified-edge mobile gateways sgw SGW-1 gtp traceoptions]
user@host# set size 50m
```

#### Related Documentation

- [Configuring General GTP Service on the S-GW on page 325](#)
- [Configuring GTP Services on the S4 Interface on page 333](#)
- [Configuring GTP Services on the S5 Interface on page 309](#)
- [Configuring General GTP Service on the S-GW on page 325](#)
- [Configuring GTP Trace Options on page 323](#)
- [Configuring S-GW GTP Traceoptions on page 338](#)
- [GPRS Tunneling Protocol \(GTP\) Overview on page 289](#)

## Configuring S-GW GTP Traceoptions

GPRS tunneling protocol (GTP) tracing operations record detailed messages about the operation of Serving Gateway (S-GW) GTP services on the MobileNext Broadband Gateway. You can trace various types of S-GW GTP operations such as errors, warnings, configuration events, and other information. You can specify which trace operations are logged by including specific tracing flags and levels.

[Table 44 on page 338](#) describes the flags relating to the S-GW GTP that you can include at the `[edit unified-edge gateways sgw gateway-name gtp traceoptions flag]` hierarchy level.

**Table 44: S-GW GTP Trace Flags**

| Flag | Description       |
|------|-------------------|
| all  | Trace everything. |



Table 44: S-GW GTP Trace Flags (*continued*)

|                  |                                         |
|------------------|-----------------------------------------|
| <b>config</b>    | Trace configuration events.             |
| <b>debug</b>     | Trace debug information                 |
| <b>decode</b>    | Trace decoding of received packets.     |
| <b>encode</b>    | Trace encoding of transmitted packets.  |
| <b>error</b>     | Trace internal or external errors.      |
| <b>events</b>    | Trace all internal or external events.  |
| <b>packet-io</b> | Trace transmitted and received packets. |
| <b>peer</b>      | Trace GTP peer-related events.          |
| <b>trackers</b>  | Trace GTP tracker-related events.       |
| <b>warning</b>   | Trace warnings.                         |

Table 45 on page 339 describes the levels you can include.

Table 45: S-GW GTP Trace Levels

| Level          | Description                                        |
|----------------|----------------------------------------------------|
| <b>all</b>     | Match all levels.                                  |
| <b>error</b>   | Match error conditions.                            |
| <b>info</b>    | Match informational messages.                      |
| <b>notice</b>  | Match conditions that should be specially handled. |
| <b>verbose</b> | Match verbose messages.                            |
| <b>warning</b> | Match warning messages.                            |

To configure tracing options for GTP operations:

1. Specify that you want to configure tracing options for GTP operations.

```
[edit unified-edge gateways sgw MBG2 gtp]
user@host# edit traceoptions
```



**NOTE:** You can use the `no-remote-trace` statement at this level to disable remote tracing capabilities.

2. Configure the filename for the trace file.

```
[edit unified-edge gateways sgw MBG2 gtp traceoptions]
user@host# set file datapath-log
```

3. (Optional) Configure the maximum size of each trace file.

```
[edit unified-edge gateways sgw MBG2 gtp traceoptions]
user@host# set file size 100m
```



**NOTE:** When a trace file (for example, `sgw-gtp-log`) reaches its maximum size, it is renamed `sgw-gtp-log.0`, then `sgw-gtp-log.1`, and so on, until the maximum number of trace files is reached. The oldest archived file is then overwritten.

4. Configure the tracing flag.

```
[edit unified-edge gateways sgw MBG2 gtp traceoptions]
user@host# set flag all
```



**NOTE:** You should use care when tracing all operations on a gateway. This can have a performance impact.

5. Configure the tracing level.

```
[edit unified-edge gateways sgw MBG2 gtp traceoptions]
user@host# set level error
```

6. View the trace file.

```
user@host# file show /var/log/sgw-gtp-log
```

#### Related Documentation

- [Configuring General GTP Service on the S-GW on page 325](#)
- [Configuring GTP Trace Options on page 323](#)
- [GPRS Tunneling Protocol \(GTP\) Overview on page 289](#)
- [Configuring S-GW Traceoptions on page 59](#)
- [Configuring S-GW Software Data Path Traceoptions on page 62](#)
- [Configuring S-GW Charging Traceoptions on page 448](#)
- [Configuring S-GW Local Persistent Storage Traceoptions on page 451](#)

---

## Example: Configuring GTP for the S-GW When Interfaces Are in different VRFs

This example describes how to configure the MobileNext Broadband Gateway Serving Gateway (S-GW) GTP interfaces when the interfaces are in different virtual routing and

forwarding (VRF) routing instances. The emphasis is on GTP configuration, and does not include many other parameters a full S-GW configuration requires.

- [Requirements on page 341](#)
- [Overview on page 341](#)
- [Configuration on page 341](#)

Requirements

This example uses the following hardware and software components:

- Junos OS Release 11.4W
- Juniper Networks MobileNext Broadband Gateway

Overview

This example describes how to configure the broadband gateway GTP interfaces when the interfaces are in different VRF routing instances. The VRFs are used to support the following configuration:

- The S11 and S5 control interfaces are in the same VRF.
- The S1-U, S12, S4, and S5 data interfaces are in the same VRF, but this VRF is not the same as the control interfaces.

Table 46: Components of the Broadband Gateway

| Property                         | Settings                                                                       | Description                               |
|----------------------------------|--------------------------------------------------------------------------------|-------------------------------------------|
| Loopback addresses               | lo0 unit 111 address 192.168.111.1/32<br>lo0 unit 112 address 192.168.112.1/32 | Identifies the device for communications. |
| Interface family                 | family inet                                                                    | The logical units belong to family inet.  |
| S11/S5 control connectivity      | VRF11-Control<br>lo0.111                                                       | VRF for S11/S5 interfaces for control     |
| S1-U/S12/S4/S5 data connectivity | VRF12-Data<br>lo0.122                                                          | VRF for S1-U/S12/S4 interfaces for data   |

Configuration

- [Configuring the Interfaces on page 342](#)
- [Enabling the Routing Instances for the VRF on page 343](#)
- [Configuring GTP Interfaces on page 344](#)

## Configuring the Interfaces

---

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set chassis redundancy graceful-switchover
set system commit synchronize
load merge /etc/config/mobility-defaults.conf
set chassis fpc 1 pic 0 apply-groups mobility
set chassis fpc 1 pic 1 apply-groups mobility
set chassis fpc 3 pic 0 apply-groups mobility
set chassis fpc 3 pic 1 apply-groups mobility
set chassis fpc 0 forwarding-packages mobility sgw
set chassis fpc 5 forwarding-packages mobilitysgw
set interfaces lo0 unit 111 family inet address 192.168.111.1/32
set interfaces lo0 unit 112 family inet address 192.168.112.1/32
```

**Step-by-Step Procedure** To configure the chassis:

1. Enable graceful restart for Routing Engine redundancy.

```
[edit]
user@pe1# set chassis redundancy graceful-switchover
```

2. Load and merge the default configuration file for the **mobility** group.

```
[edit]
user@pe1# load merge /etc/config/mobility-defaults.conf
```

3. Configure the **mobility** group on the session DPCs.

```
[edit]
user@pe1# set chassis fpc 1 pic 0 apply-groups mobility
user@pe1# set chassis fpc 1 pic 1 apply-groups mobility
user@pe1# set chassis fpc 3 pic 0 apply-groups mobility
user@pe1# set chassis fpc 3 pic 1 apply-groups mobility
```



**NOTE:** You must include every services PIC configured with the **jservices-mobile** package at the **[edit unified-edge gateways sgw gateway-name system anchor-spics]** hierarchy level on the broadband gateway. If you do not include the services PIC as an anchor interface, then the services PIC will not be used by the broadband gateway.

4. Configure the interface DPC or MPC at the FPC level.

```
[edit]
user@pe1# set chassis fpc 0 forwarding-packages mobility sgw
user@pe1# set chassis fpc 5 forwarding-packages mobility sgw
```



**NOTE:** You must include every Packet Forwarding Engine configured with the `sgw` forwarding package at the `[edit unified-edge gateways sgw gateway-name system anchor-pfes]` hierarchy level on the broadband gateway. If you do not specify the Packet Forwarding Engine as an anchor interface, then the Packet Forwarding Engine will not be used by the broadband gateway.

5. Configure loopback interfaces.

[edit]

```
user@pe1# set interfaces lo0 unit 111 family inet address 192.168.111.1/32
user@pe1# set interfaces lo0 unit 112 family inet address 192.168.112.1/32
```

### Enabling the Routing Instances for the VRF

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

[edit]

```
set routing-instances VRF11-Control instance-type vrf
set routing-instances VRF11-Control interface lo0.111
set routing-instances VRF11-Control route-distinguisher 192.168.111.1:111
set routing-instances VRF11-Control vrf-target target:1:111
set routing-instances VRF11-Control vrf-table-label
set routing-instances VRF12-Data instance-type vrf
set routing-instances VRF12-Data interface lo0.112
set routing-instances VRF12-Data route-distinguisher 192.168.112.1:112
set routing-instances VRF12-Data vrf-target target:1:112
set routing-instances VRF12-Data vrf-table-label
```

#### Step-by-Step Procedure

To configure the routing instance for the VRF used:



**BEST PRACTICE:** For GTP traffic, use the `vrf-table-label` option when configuring the routing instances.

1. Configure the VRF routing instances for GTP traffic.

[edit]

```
user@pe1# set routing-instances VRF11-Control instance-type vrf
user@pe1# set routing-instances VRF11-Control interface lo0.111
user@pe1# set routing-instances VRF11-Control route-distinguisher 192.168.111.1:111
user@pe1# set routing-instances VRF11-Control vrf-target target:1:111
user@pe1# set routing-instances VRF11-Control vrf-table-label
user@pe1# set routing-instances VRF12-Data instance-type vrf
user@pe1# set routing-instances VRF12-Data interface lo0.112
user@pe1# set routing-instances VRF12-Data route-distinguisher 192.168.112.1:112
user@pe1# set routing-instances VRF12-Data vrf-target target:1:112
user@pe1# set routing-instances VRF12-Data vrf-table-label
```

### Configuring GTP Interfaces

---

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge gateways sgw MBG1 gtp s11 interface lo0.111
set unified-edge gateways sgw MBG1 gtp s5 control interface lo0.111
set unified-edge gateways sgw MBG1 gtp s1u interface lo0.112
set unified-edge gateways sgw MBG1 gtp s12 interface lo0.112
set unified-edge gateways sgw MBG1 gtp s4 data interface lo0.112
set unified-edge gateways sgw MBG1 gtp s5 data interface lo0.112
```

**Step-by-Step Procedure** To configure GTP interfaces:

1. Configure the GTP interfaces for the broadband gateway called MBG1.

```
[edit]
user@pe1# edit unified-edge gateways sgw MBG1 gtp
```

2. Specify the appropriate loopback interface associated with the VRF routing instance for the S11 and S5 control interfaces and S1-U, S12, S4, and S5 data interfaces.

```
[edit unified-edge gateways sgw MBG1 gtp]
user@pe1# set s5 control interface lo0.111
user@pe1# set s11 interface lo0.111
user@pe1# set s1u interface lo0.112
user@pe1# set s12 interface lo0.112
user@pe1# set s4 data interface lo0.112
user@pe1# set s5 data interface lo0.112
```

**Related Documentation**

- [Configuring General GTP Service on the S-GW on page 325](#)
- [Configuring GTP Trace Options on page 323](#)
- [GPRS Tunneling Protocol \(GTP\) Overview on page 289](#)

## PART 7

# Policy and Charging Enforcement Function Configuration

- [Policy and Charging Enforcement Function Overview on page 347](#)
- [Configuring Policy and Charging Enforcement Function on page 365](#)





# Policy and Charging Enforcement Function Overview

- [Policy and Charging Enforcement Function Overview on page 347](#)
- [Policy and Charging Control Rules Overview on page 349](#)
- [Application-Aware Policy and Charging Control Rules Overview on page 353](#)
- [APPID Feature Overview on page 355](#)
- [Understanding How Dynamic and Static Policy and Charging Control Rules Are Provisioned on page 359](#)
- [Bearer Binding Overview on page 361](#)
- [Understanding Event Triggers on page 363](#)

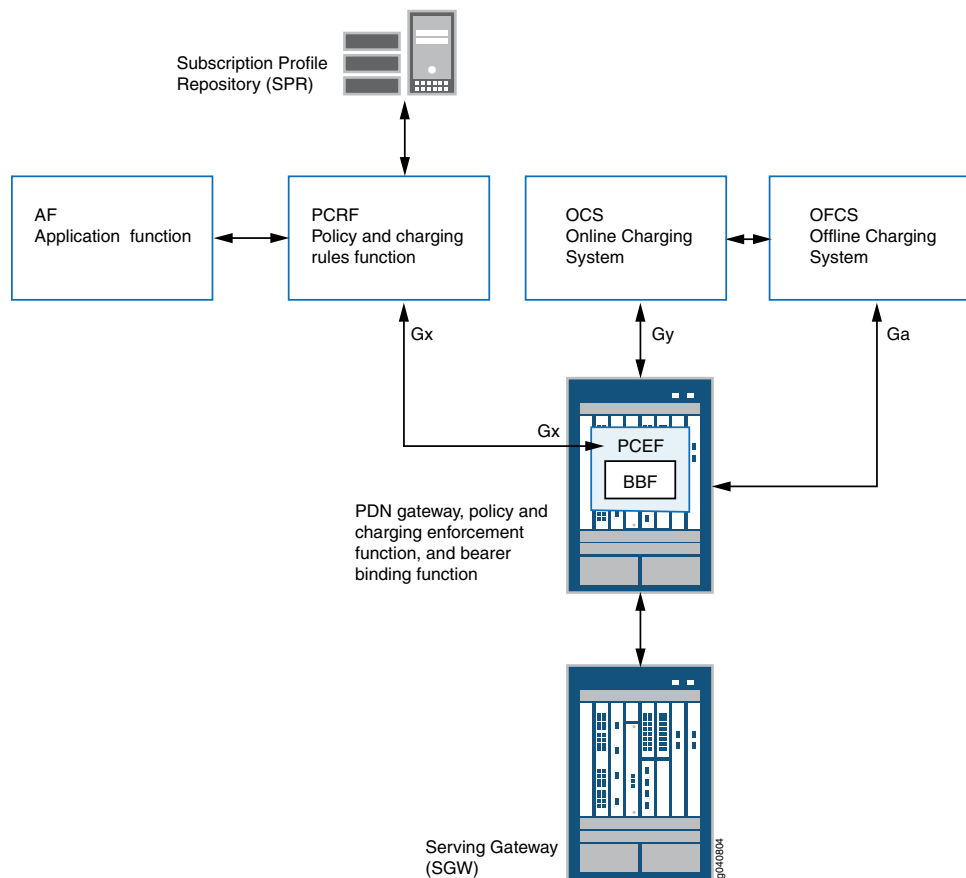
## Policy and Charging Enforcement Function Overview

---

The policy and charging enforcement function (PCEF) enforces policy decisions that are received from the policy and charging rules function (PCRF) and provides the PCRF with subscriber and access information over the Gx interface, which connects the PCEF and the PCRF. For dynamic policies, the PCEF can also act upon the messages received from the PCRF to install, modify, or remove Policy and Charging Control (PCC) rules. For static policies, the PCEF enforces policy decisions with no interaction from the PCRF and no Gx interface support.

The PCEF is part of a complete broadband gateway configuration, including online and offline charging, and quality-of-service (QoS) determination. The PCEF interacts with the internal charging function, which, in turn, interacts with the Online Charging System (OCS), which provides credit management for prepaid charging, and reports resource usage to the Offline Charging System (OFCS). [Figure 47 on page 348](#) shows the overall architecture for the gateway components and the functional groupings for policy and charging.

Figure 47: Architecture for Policy and Charging Enforcement Function



A PCEF configuration on the MobileNext Broadband Gateway comprises the following filters, rules, and profiles:

- Service data flow filters—Provides detection of IP flows based on source IP, destination IP, source port, destination port, Layer 4 protocol (UDP and TCP), applications (for example, BitTorrent and HTTP), and nested applications (for example, YouTube and Facebook). A service data flow filter is specified in the **from** clause of the PCC rules to detect uplink service flows, downlink service flows, or both.
- PCC action profile—Defines the QoS, charging, and gating controls to apply to a bearer. A PCC action profile is specified in the **then** clause of the PCC rule.
- PCC rules—Defines the QoS, charging, and gating control for specified traffic flows between the Packet Data Network Gateway (P-GW) and the user equipment (UE). A PCC rules configuration includes service data flow filters and a PCC action profile.
- (Optional) PCC rulebase—Defines a group of PCC rules, each of which are assigned a precedence for specified traffic flows between the P-GW and the user equipment (UE).
- (Optional) Event-trigger profile—Provides event notification to the PCRF when an event-trigger event occurs on the network, such as radio access technology (RAT)

change, or Serving Gateway Support Node (SGSN) change. An event-trigger profile can be configured in the PCEF profile with dynamic policy control.

- PCEF profile—Defines either static policies or dynamic policies. A PCEF profile configured with static policy control requires predefined PCC rules, PCC rulebases, or both. A PCEF profile configured with dynamic policy control requires a Diameter Gx profile and, optionally, event-trigger profiles and predefined PCC rules, PCC rulebases, or both.

**Related  
Documentation**

- [Policy and Charging Control Rules Overview on page 349](#)
- [Application-Aware Policy and Charging Control Rules Overview on page 353](#)
- [Understanding How Dynamic and Static Policy and Charging Control Rules Are Provisioned on page 359](#)
- [Understanding Event Triggers on page 363](#)

---

## Policy and Charging Control Rules Overview

In the Policy and Charging Control (PCC) architecture, the policy and charging rule function (PCRF) is the central entity that makes policy and charging decisions based on input from different sources, including mobile operator configuration, user subscription information, services information, and so forth. The PCC decisions are then communicated to the policy and charging enforcement function in the form of PCC rules, which contain service data flow (SDF) information that allows identification of IP traffic, charging parameters that are used to charge this traffic, and quality-of-service (QoS) parameters to be applied to the IP traffic that the SDF filters identify. PCC rules can also be statically configured in the PCEF and then dynamically referenced by the PCRF through the Gx interface.

This topic includes the following sections:

- [Understanding Service Data Flow Filters on page 349](#)
- [Policy and Charging Control on page 351](#)
- [PCC Rules Under Static Policy Control on page 352](#)
- [PCC Rules Under Dynamic Policy Control on page 352](#)
- [Static-Gx Rules on page 353](#)
- [Policing of Subscriber Traffic on page 353](#)

### Understanding Service Data Flow Filters

Service data flow (SDF) filters (flow identifiers) are configured in PCC rules to classify IP packets to a service data flow. SDF filters in the PCC rules enforce transport of uplink and downlink IP flows in the appropriate IP CAN bearer. If the IP packet matches the SDF filter, and the gate of the corresponding rule is open, the packet is forwarded to its destination.

To configure Layer 3 or Layer 4 SDF filters, you specify one or more of the following parameters to detect IP packet flows:

- Source IP address
- Destination IP address
- Source port
- Destination port
- Layer 4 protocol (UDP or TCP)

To configure application-aware SDF filters, you can specify one or more of the following parameters to detect IP packet flows:

- application—Specifies the name of an application, for example, HTTP.
- nested-application—Specifies encapsulated application types (with different application signatures) that are running on the same Layer 7 protocols. For example, both Facebook and Yahoo Messenger can run over HTTP, but to identify them as two different applications, the application layer is divided into two layers: Layer 7 applications and Layer 7 protocols.
- application-group—Specifies the name of an application group, which can be used to process a number of applications or subgroups at the same time.

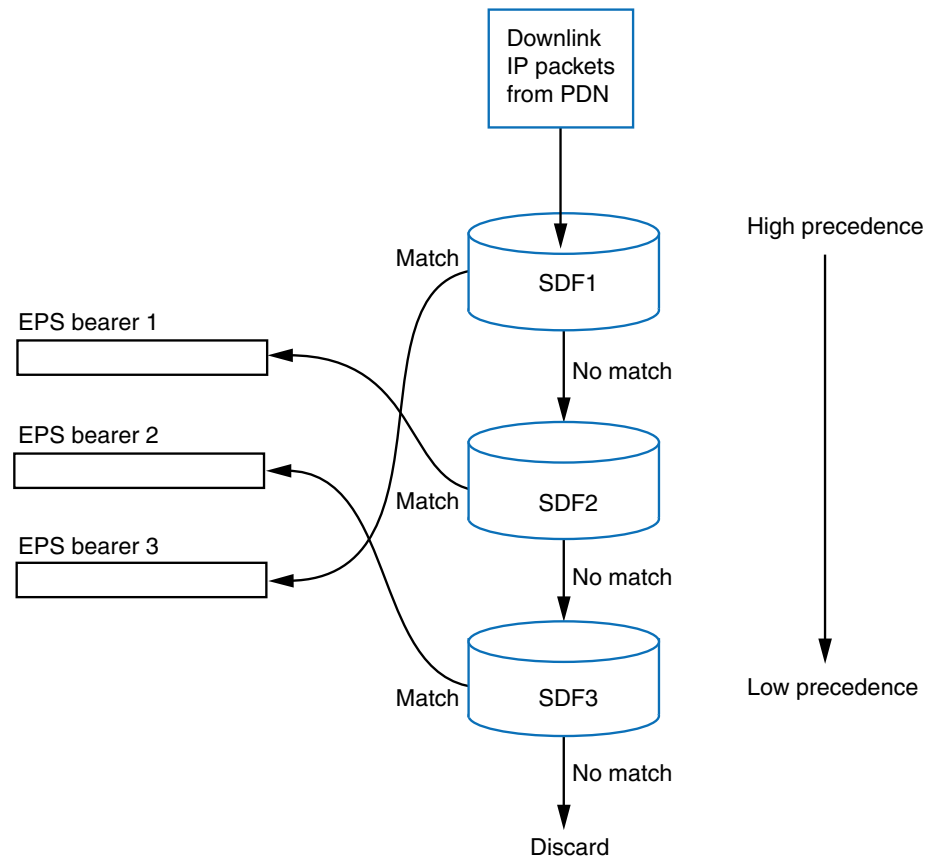


**NOTE:** Application-aware PCC rules that reference specified applications can include wildcard or specific Layer-3 SDF filters, Layer-4 SDF filters, or both.

---

All IP packets that match an SDF filter (flow identifier, application, nested-application, or application-group) are designated a service data flow. [Figure 48 on page 351](#) shows the process by which the configured SDF filters direct IP packets to an appropriate bearer.

Figure 48: Service Data Flow Filtering of Downlink IP Packets



0080705

SDF filters are evaluated in order of precedence assigned to the PCC rules within the session. For example, when multiple rules are associated with a bearer, the SDF filters in PCC rules of higher precedence are evaluated prior to the SDF filters in PCC rules of a lower precedence.

**NOTE:**

- The precedence assigned must be unique among the configured PCC rules.
- The higher the precedence value the lower the precedence and vice-versa; for example, if a PCC rulebase has two PCC rules with precedence 5 and 10 respectively, the PCC rule with precedence 5 is evaluated first and then the PCC rule with precedence 10 is evaluated.

## Policy and Charging Control

A PCC rule configuration includes an action profile that defines the quality-of-service (QoS), charging, and gating control to apply to a service data flow. A PCC action profile can be configured and used in one or more PCC rules to provide the following functionality:

- **QoS control**—Allows the PCRF to specify the QoS treatment for an SDF. QoS can include QoS Class Identifier (QCI), allocation retention priority (ARP), maximum bit rate (MBR), guaranteed bit rate (GBR), and preemption vulnerability or capability. The PCEF enforces the QoS control by establishing or modifying bearers and enforcing bit rates for service sessions.
- **Charging control**—The PCRF determines whether online or offline charging is appropriate for a given service session. The PCEF, in turn, enforces that decision by interacting with the charging systems and collecting charging data. The PCRF also controls the measurement method (volume, duration, volume/duration, or event-based) to use.
- **Gating status**—Specifies whether IP packets associated with an SDF should be blocked or allowed. The PCEF allows or blocks IP packets associated with an SDF to ensure that the SDF does not violate the authorized QoS. The PCRF makes the gating decisions (open or closed), which the PCEF enforces on a per SDF basis.

## PCC Rules Under Static Policy Control

*Static* PCC rules (policies) are provisioned by the PCEF with no interaction from the PCRF and no Gx interface support. Static policies can be predefined on the MobileNext Broadband Gateway and are activated by the PCEF when a PCEF profile is applied to an APN or service-selection profile.

## PCC Rules Under Dynamic Policy Control

*Dynamic* PCC rules are provisioned by the PCRF to the PCEF and are carried over the Gx interface using Diameter AVPs. The PCRF is central in making policy and charging control decisions and can activate, modify, or deactivate a dynamic rule at any time. The PCRF can provision the complete PCC rules or provision the name of predefined rules (static-Gx policies).

The PCRF can make its policy and charging control decisions based different sources, including:

- Subscription information for a UE that is received from the SPR
- Operator configuration in the PCRF
- Information from the access network about the access technology

The broadband gateway supports the following operations for dynamic PCC rules:

- **Install or modify**—The **Charging-Rule-Install** AVP is used to install a PCC rule that is not already installed or modify an existing rule on the broadband gateway.
- **Remove**—The **Charging-Rule-Remove** AVP is used to remove a PCC rule that is already installed.

The containers for the PCC rules are named **Charging-Rule-Definition**. Multiple **Charging-Rule-Definition** containers can be sent within a **Charging-Rule-Install** or **Charging-Rule-Remove**, each of which is applied per bearer.

## Static-Gx Rules

Static Gx PCC rules are configured on the PCEF but provisioned by the PCRF over the Gx interface using Diameter AVPs. The PCRF provides the name of the local PCC rule or group of PCC rules to be activated or deactivated. The broadband gateway supports the following operations for static Gx rules:

- Install or modify—**Charging-Rule-Install** AVP is used to install a PCC rule that has not been installed or modify an existing rule on the broadband gateway.
- Remove—**Charging-Rule-Remove** AVP is used to remove a PCC rule that is already installed.

## Policing of Subscriber Traffic

For 3G and 4G GBR bearers, the maximum bit rate (MBR) and guaranteed bit rate (GBR) is applied per PCC rule.

For non-GBR bearers, the following behavior applies:

- For 3G Release 9 and 4G subscriber traffic, all non-GBR bearers associated with a session share the APN-AMBR value, which defines the total bit rate that is allowed for all non-GBR bearers associated with an APN.
- For 3G pre-Release 9 subscriber traffic, a specific QoS is associated with a bearer, and policing is performed at the bearer level.

### Related Documentation

- [Application-Aware Policy and Charging Control Rules Overview on page 353](#)
- [Policy and Charging Enforcement Function Overview on page 347](#)
- [Understanding Event Triggers on page 363](#)
- [Understanding How Dynamic and Static Policy and Charging Control Rules Are Provisioned on page 359](#)

---

## Application-Aware Policy and Charging Control Rules Overview

The policy and charging enforcement function (PCEF) supports Layer 3 and Layer 4 policy and charging control (PCC) rules as well as application-aware PCC rules that use deep packet inspection (DPI) to support policies for Layer 7 and higher-layer application traffic. For application-aware PCC rules, the PCRF can only refer PCC rules or rulebases (static Gx policies) that are statically configured on the MobileNext Broadband Gateway.

This topic covers:

- [Understanding Application-Aware PCEF Services on the Broadband Gateway on page 354](#)
- [Use Case for Application-Aware PCEF Service on page 354](#)
- [Junos OS Services Package Requirements for Application-Aware PCEF on page 355](#)

## Understanding Application-Aware PCEF Services on the Broadband Gateway

To enforce Layer 3 and Layer 4 PCC rules, the Packet Forwarding Engine inspects uplink and downlink subscriber traffic on an access point name (APN). To enforce application-aware PCC rules, the policy and charging enforcement function (PCEF) is applied as a service on the APN (MIF interface) to indicate to the Packet Forwarding Engine that traffic should be directed to the Junos OS services PIC that hosts the PCEF service. When subscriber traffic is redirected to the services PIC, processing is completed and the appropriate policies are applied as a service on the MIF interface associated with an APN.

At the Junos OS services PIC, the application-identification engine inspects traffic to match against a database of application signatures, which are either imported from a Juniper intranet or extranet server or are configured from the command-line interface (CLI). An application signature typically identifies a unique type of application, for example, YouTube video, or a set of applications, for example, streaming audio.

The PCEF service takes information provided by the application-identification engine and retrieves the database of PCC rules to determine the appropriate policies and charging actions to apply to the specified application-aware traffic flow.

An application-aware service set must be configured (and applied on the APN interface) to link the application-identification engine and PCEF service together. For this release, a PCEF (services) profile includes no configurable attributes; however, to reference the PCEF service in a service set, you must configure the PCEF profile.

For mobile subscribers, the Packet Forwarding Engine handles GPRS Tunneling Protocol (GTP) encapsulation and decapsulation even when subscriber traffic might require processing by an application-aware service. In the uplink (Gn to Gi) direction, decapsulated subscriber traffic is sent to the services PIC. In the downlink (Gi to Gn) direction, the incoming Internet traffic is sent to the services PIC, and after the PCEF service, is redirected to the Packet Forwarding Engine for GTP encapsulation towards a Serving Gateway Support Node (SGSN) or Serving Gateway (SGW).

## Use Case for Application-Aware PCEF Service

An application-aware PCEF service supports both online and offline charging, based on the application signatures. For example, you might configure an application-aware PCEF service to define different Internet walled-garden server URLs in the application-identification engine, and assign these URL signatures to different PCC rules to provide differentiated charging.

The following steps outline how an operator might configure an application-aware PCEF service to provide free access to social networking sites during off-peak hours:

- Define the URL signatures for the targeted social networking sites.
- Define the PCC rules by specifying different rating groups for these URL signatures.
- The Junos OS PCEF service reports charging data for traffic that matches the URL signatures to the internal charging system.



- The Junos OS PCEF service reports charging data for traffic that matches the URL signatures to the internal charging system.
- The internal charging system interacts with the Online Charging System (OCS) or Offline Charging System (OFCS) depending on the characteristics of the rating group.
- Operator billing infrastructure uses this rating group to bypass or apply a different billing rate to the subscriber traffic that is reported for the particular rating group.



**NOTE:** The Layer 3 or Layer 4 based PCEF on the Packet Forwarding Engine does not account for traffic that is redirected to the Junos OS services plane for application-aware inspection, so subscriber traffic is protected from being double accounted for both a Layer 3 or Layer 4 rule and application-aware rule or rating group.

## Junos OS Services Package Requirements for Application-Aware PCEF

To provide application-aware policy enforcement on the network, the MobileNext Broadband Gateway uses the following services packages to perform deep packet inspection (DPI) on the Junos OS services plane (services PIC):

- `jservices-appid`—The application-identification engine on the SRX Series or MX Series platform, which inspects and detects application traffic.
- `jservices-mss`—The mobile subscriber services package on the MX platform, which provides mobile subscriber awareness and user equipment (UE) session information to the Junos OS services plane.
- `jservices-pcef`—The PCEF service package, which provides application-aware PCEF.

### Related Documentation

- [Understanding How Dynamic and Static Policy and Charging Control Rules Are Provisioned on page 359](#)
- [Policy and Charging Enforcement Function Overview on page 347](#)
- [APPID Feature Overview on page 355](#)

## APPID Feature Overview

The APPID (application identification) feature is a Junos OS feature that identifies applications as constituents of application groups in TCP/UDP/ICMP traffic.

The MobileNext Broadband Gateway supports the following APPID features:

- [Application Tracking \(AppTrack\) on page 356](#)
- [Custom Application Signatures on page 356](#)
- [Signature Groups on page 357](#)
- [Heuristics-Based Detection on page 358](#)
- [Nested Application Identification on page 358](#)

## Application Tracking (AppTrack)

Juniper Networks provides predefined application signatures that detect TCP and UDP applications running on non-standard ports. Identifying these applications provides data for application tracking (AppTrack). A PCC rule that includes application-aware SDF filters also uses the application data to perform actions (charging, blocking, rate-limiting, redirecting) on the application traffic.



**NOTE:** The broadband gateway does not support Application Firewall (AppFw), Application QoS (AppQoS), Application DDoD, or Intrusion Detect Prevention (IDP).

Juniper Networks provides frequent updates to the predefined application signature package database and makes these updates available to subscribers on the Juniper Networks website. This package includes signature definitions of known application objects that can be used to identify applications for tracking, firewall policies, quality of service prioritization, and IDP. The application signature package database contains application objects such as FTP and DNS as well as nested applications that operate over an HTTP protocol, such as Facebook, Kazaa, and instant messenger programs.

Before you configure application identification, application firewall policy, or AppTrack, you must download and install the application signature package, which is included in the default IDP installation and does not need to be downloaded separately.

If you do not plan to use application identification, you can execute the following commands to extract the application portion of the IDP signature database and install it as the application signature database:

- **request services application-identification download**
- **request services application-identification install**

## Custom Application Signatures

Application identification supports user-defined custom application signatures, nested application signatures, and signature groups. Custom application signatures are unique to your environment and are not part of the predefined application package. When you update or uninstall the application package, the custom signatures and signature groups are not modified or removed.



**NOTE:** The uninstall operation will fail if any active security policies, custom application signatures, or signature groups reference predefined application signatures or signature groups in the Junos OS configuration.

To create custom application signatures, use the CLI to specify a name, the protocol and port where the application runs, the signature pattern, and match criteria. For ease of

use, copy a similar predefined application signature or group, and modify the characteristics so that it identifies the unique application running in your environment.

You can view application signatures and application signature groups by using the **show services application-identification application** and **show services application-identification group** commands.

You can copy a predefined application signature or signature group to use as a model by entering the **request services application-identification application copy** or the **request services application-identification group copy** command. With this command, your copy is automatically named by replacing the “junos” prefix with the prefix “my”. (The “junos” prefix is reserved for predefined application signatures and groups.) You can copy the same predefined application signature and signature group only once. Duplicate custom signatures and groups are not allowed. Rename your custom application signature or signature group to a unique name appropriate to your environment.

For additional information about MobileNext Broadband Gateway support for signature groups, see [Understanding Application Grouping for Junos OS Application Identification](#).

## Signature Groups

In Junos OS, application grouping lets you group multiple applications under a single name to improve accuracy and consistency in policy definition. Both predefined and user-defined applications can be grouped together.

The hierarchy of application groups resembles a tree structure with associated applications as the leaf nodes. The group any refers to the root node. The group unassigned is always situated one level from the root and initially contains all applications. When a group is defined, applications are assigned from the unassigned group to the new group. When a group is deleted, its applications are moved back to the unassigned group.

Applications can be assigned to a group or can remain unassigned, but they cannot be assigned to more than one group. There is no specific limitation on the number of applications assigned to a single group or on the number of application groups that can be configured for a device.

All predefined application groups have the prefix “junos” in the application group name to prevent naming conflicts with custom application groups. You cannot modify the list of applications within a predefined application group. However, you can copy a predefined application group to use it as a template for creating a custom application group.

To customize a predefined application group you must first disable the predefined group. Note that a disabled predefined application group remains disabled after an application database update. You can then use the operational command **request services application-identification group** to copy the disabled predefined application group. The copied group is placed in the configuration file, and the prefix “junos” is changed to “my”. At this point, you can modify the list of applications in “my” application group and rename the group with a unique name.

To reassign an application from one custom group to another, you must remove the application from its current custom application group, and then reassign it to the other.

See the *Junos OS CLI Reference* for information about using the **request services application-identification** commands.

## Heuristics-Based Detection

Peer-to-peer applications such as Skype contain encrypted data packets. The SRX devices cannot identify the encrypted data packets with the current application signatures, which are based on regular expression patterns. Heuristics are used to detect such traffic and to improve the detection rate. To enable detection of encrypted peer-to-peer applications, you can use the following command:

```
set services application-identification enable-heuristics
```

Junos OS detects encrypted peer-to-peer traffic on TCP and UDP.

If a session cannot be identified as known encrypted peer-to-peer traffic, you can assign the session to a special application named *junos:unspecified-encrypted*. Application firewall can configure a policy on the application that is similar to other dynamic applications.

## Nested Application Identification

Greater use of application protocol encapsulation requires support for the identification of multiple applications running on the same Layer 7 protocols. For example, applications such as Facebook and Yahoo Messenger can both run over HTTP, but there is a need to identify them as two different applications running on the same Layer 7 protocol. In order to do this, the current application identification layer is split into two layers: Layer 7 nested applications and Layer 7 protocols.

The included predefined application signatures are created to detect the Layer 7 nested applications, whereas the existing Layer 7 protocol signatures, such as FTP and HTTP, still function in the same manner. You can use these predefined application signatures in attack objects.

The nested application identification module detects nested applications based on the patterns in HTTP contexts. However, some HTTP sessions are encrypted in SSL, also called Transport Layer Security (TLS).

Application identification can also extract the server name information or the server certification from the TLS or SSL sessions.

### Related Documentation

- [Application-Aware Policy and Charging Control Rules Overview on page 353](#)
- [Configuring Policy and Charging Enforcement Function Services for Application-Aware Traffic on page 365](#)

## Understanding How Dynamic and Static Policy and Charging Control Rules Are Provisioned

Located between the policy and charging rules function (PCRF) and policy control enforcement function (PCEF), the Gx interface is used to provision or remove Policy and Charging Control (PCC) rules from the PCRF to the PCEF, and provide notification of traffic-plane events from the PCEF to the PCRF.

This topic includes the following sections:

- [Understanding How Rules Are Provisioned on the Gx Interface on page 359](#)
- [Provisioning of Dynamic Policies on page 359](#)
- [Provisioning of Predefined Static Policies on page 361](#)

### Understanding How Rules Are Provisioned on the Gx Interface

The Gx interface provides charging and policy control by applying attribute-value pairs (AVPs) relevant to the application.

The PCRF collects and compares subscriber and application data, authorizes quality-of-service resources, and provides instructions (the PCC rules) for transporting subscriber traffic, as follows:

1. To determine the policy decisions that form the policy rules, the PCRF evaluates session information, subscription data for user equipment (UE) from the Subscription Profile Repository (SPR), operator-defined service policies, and other information from the access network about the access technology.
2. The PCRF sends the PCC rules (either the rules or name of the rules) to the PCEF, which enforces policy decisions based on the rules that are received.



**NOTE:** If the PCC rules indicate that online charging will apply, the PCEF notifies the Online Charging System (OCS), via the Gy interface, and requests credit based on the measurement method that the PCC rules specifies. If the PCC rules indicate that offline charging will apply, the PCEF notifies the internal charging module, which will collect usage data that is then forwarded to the Offline Charging System (OFCS).

3. The PCEF installs the PCC rules and performs bearer binding to ensure that the traffic for this service receives the required QoS and charging treatment. Bearer operations (session modifications) might require a Create Bearer request or Modify Bearer request.
4. Data is transported across the network, and the PCEF performs service data flow (SDF) detection to detect the IP flow for this service.

### Provisioning of Dynamic Policies

Dynamic policies include both *dynamic* policies, which are provisioned by the PCRF to the PCEF, and are carried over the Gx interface, and *static* Gx policies, which are predefined

rules (configured on the PCEF) that are dynamically controlled (activated and deactivated) by the PCRF. The PCRF is central in making Policy and Charging Control (PCC) decisions and can activate, modify, or deactivate a dynamic rule at any time.

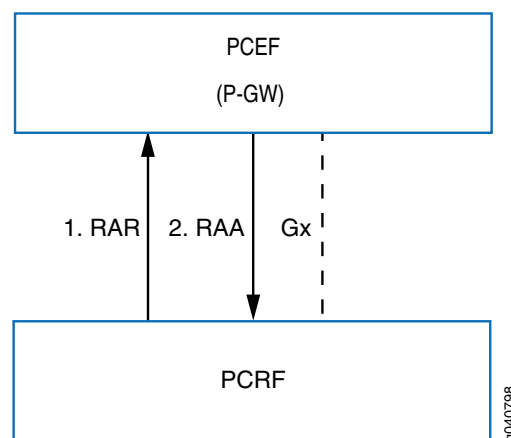


**NOTE:** The P-GW gives precedence to dynamic policies sent by the PCRF over static (predefined) policies that are configured on the PCEF.

The PCRF uses one of the following procedures to specify the PCC rules that the PCEF will apply:

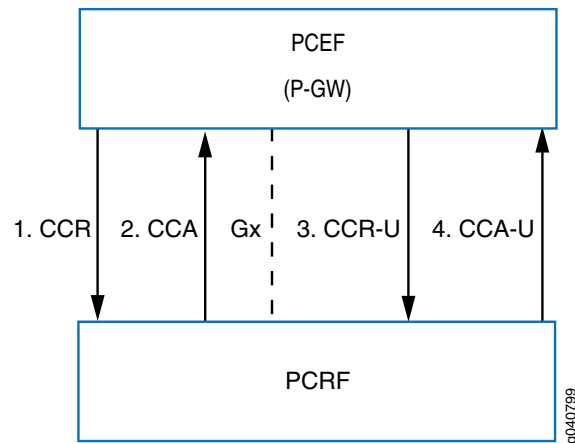
- **Push mode**—Applies when the PCRF decides to provision PCC rules without obtaining a request from the PCEF. The PCRF sends a Re-Authorization Request (RAR) to the PCEF based on information sent to the PCRF via the Rx interface or in response to a trigger within the PCRF. Because the PCC rules were not requested by the PCEF, the PCRF includes these PCC rules in a RAR message, and no Credit Control Request (CCR) or Credit Control Answer (CCA) messages are triggered by the RAR. [Figure 49 on page 360](#) shows the message flow for a push procedure.

**Figure 49: Message Flow for Push Mode**



- **Pull mode**—Applies when the PCEF requests PCC rules from the PCRF. The PCEF sends a Credit Control Request (CCR) message for PCC rules to the PCRF, and the PCRF provisions the appropriate PCC rules in the Credit Control Answer (CCA). [Figure 50 on page 361](#) shows the message flow for a pull procedure.

Figure 50: Message Flow for Pull Mode



A pull procedure is initiated during IP Connectivity Access Network (IP-CAN) session establishment (CCR-Init) or IP-CAN session modification (CCR-Update).

An IP-CAN session modification is initiated under the following conditions:

- A new IP-CAN bearer is being established, modified, or terminated.
- UE-initiated resource modification bearer is being established, modified, or terminated.
- An event-trigger event occurs, such as Radio Access Technology (RAT) change.

## Provisioning of Predefined Static Policies

*Static* PCC rules are predefined rules that are provisioned by the PCEF with no interaction from the PCRF and no Gx interface support. Because a static policy is not controlled by the PCRF, a static policy is typically applied to all subscriber traffic on a given APN, and activated or deactivated locally on the P-GW.

- Related Documentation**
- [Policy and Charging Control Rules Overview on page 349](#)
  - [Understanding Event Triggers on page 363](#)

## Bearer Binding Overview

Bearer binding refers to the association between a bearer and the Policy and Charging Control (PCC) rules. To ensure that subscriber packets receive the appropriate quality of service (QoS), charging, and gating control, a PCC rule is mapped to a corresponding bearer in the access network. Bearer binding is performed by the policy and charging enforcement function (PCEF).

When the policy and charging rules function (PCRF) provides details about the active PCC rules to the PCEF, the PCEF determines if an existing bearer in the access network can be used. If no bearer exists with the corresponding combination of QoS Class Identifier

(QCI) and allocation retention priority (ARP) values specified in the PCC rules, then the PCEF initiates the creation of new bearers.



**NOTE:** The ARP value specifies the priority level, preemption-vulnerability, and preemption-capability, so if the combination of ARP values specified in the PCC rules is not also specified in an existing bearer (with the same QCI) on the access network, a new bearer is installed or activated with the same QCI and ARP values.



**NOTE:** To provide a match with an application-aware PCC rule, the PCEF service must defer bearer binding until the HTTP (or relevant application layer) subscriber packets are detected on the service data flow. However, after the match is completed and the traffic is mapped to a dedicated bearer, the service data flow cannot be remapped to a different dedicated bearer.

The bearer binding function can trigger any combination of the following bearer requests:

- Create bearer requests—Triggered when a PCC rule arrives with unique QCI/ARP values (no existing bearer in the session has the same combination of QCI/ARP values).
- Update bearer requests can be triggered when the following changes occur:
  - Traffic flow template for the bearer has changed (SDF filters are added or removed).
  - Precedence for PCC rules has changed.
  - APN-AMBR is updated.
  - MBR/GBR values of a GBR bearer are modified.
- Delete bearer requests—Triggered when all PCC rules associated with a dedicated bearer are deleted.

**Related  
Documentation**

- [Policy and Charging Control Rules Overview on page 349](#)
- [Understanding How Dynamic and Static Policy and Charging Control Rules Are Provisioned on page 359](#)
- [Policy and Charging Enforcement Function Overview on page 347](#)
- [Understanding Event Triggers on page 363](#)



---

## Understanding Event Triggers

---

You can configure event triggers on the policy and charging enforcement function (PCEF) so that the PCEF notifies the policy and charging rules function (PCRF) about changes in the access network. By default, the PCEF enables any event triggers that are received from the PCRF in a Credit Control Answer (CCA) or Re-Authorization Request (RAR) message. When you configure event triggers on the PCEF, the PCEF adds these PCEF configured event triggers to the PCRF provisioned event triggers.

When an event occurs that matches an event trigger configured on the PCEF or provisioned from the PCRF, the PCEF reports the event to the PCRF. In some circumstances, the PCRF might require information from the P-GW/GGSN or PCEF in order to make a policy decision, for example, when the access technology in use by the user equipment (UE) changes, or a subscriber leaves the home network and is roaming, or the authorized guaranteed bit rate (GBR) cannot be supported over the radio link.

The PCEF also supports the unconditional (implicit) event triggers, in which the PCEF unconditionally reports certain events to PCRF without any need for configuration of the event triggers on the PCEF or receipt of event triggers from the PCRF) in a Credit Control Answer (CCA) or Re-Auth Request (RAR) message.

This topic includes the following sections:

- [Implicit Event Triggers on page 363](#)
- [Configurable PCEF-Enabled Event Triggers on page 363](#)

### Implicit Event Triggers

Implicit event triggers define the events that the PCEF must report to the PCRF, even though the PCRF does not explicitly subscribe to these events.

The MobileNext Broadband Gateway includes the following implicit event triggers:

- QOS\_CHANGE
- LOSS\_OF\_BEARER
- RECOVERY\_OF\_BEARER
- DEFAULT\_EPS\_BEARER\_QOS\_CHANGE

### Configurable PCEF-Enabled Event Triggers

To configure event triggers that identify the events that the PCEF must report to the PCRF, you must explicitly include the event triggers in an event-trigger profile. The following event triggers can be configured on the PCEF:

- IP\_CAN\_CHANGE
- PLMN\_CHANGE
- RAT\_CHANGE

- RAI\_CHANGE
- SSGN\_CHANGE
- TFT\_CHANGE
- UE\_TIMEZONE\_CHANGE
- USER\_LOCATION\_CHANGE

**Related  
Documentation**

- [Configuring Event Trigger Profiles on page 373](#)
- [Policy and Charging Control Rules Overview on page 349](#)
- [Understanding How Dynamic and Static Policy and Charging Control Rules Are Provisioned on page 359](#)

## CHAPTER 18

# Configuring Policy and Charging Enforcement Function

- [Configuring Policy and Charging Enforcement Function Services for Application-Aware Traffic on page 365](#)
- [Configuring Service Data Flow Filters \(Flow Identifiers\) on page 367](#)
- [Configuring Policy and Charging Control Action Profiles on page 369](#)
- [Configuring Layer 3 and Layer 4 Policy and Charging Control Rules on page 370](#)
- [Configuring Application-Aware Policy and Charging Control Rules on page 371](#)
- [Configuring a Policy and Charging Control Rulebase on page 372](#)
- [Configuring Event Trigger Profiles on page 373](#)
- [Configuring a Policy and Charging Enforcement Function Profile for Dynamic Policies on page 375](#)
- [Configuring a Policy and Charging Enforcement Function Profile for Static Policies on page 377](#)
- [Tracing PCEF Operations on page 378](#)
- [Example: Configuring Policy and Charging Enforcement Function With Layer 3 and Layer 4 Policy and Charging Control Rules on page 379](#)
- [Example: Configuring Policy and Charging Enforcement Function with Application-Aware Policy and Charging Control Rules on page 397](#)

## Configuring Policy and Charging Enforcement Function Services for Application-Aware Traffic

---

The MobileNext Broadband Gateway supports application-aware service data flows (SDFs) in Policy and Charging Control (PCC) rules to inspect traffic for mobile subscribers accessing Web-based services. Before you configure application-aware PCC rules, you must configure a PCEF profile as a service for an access point name (APN) so that all traffic flowing through the APN is inspected for application-aware based charging and policy enforcement.

Before you configure a PCEF profile as a service for a broadband gateway APN, complete the following tasks:

- Configure the chassis of the broadband gateway
- Configure the interfaces of the broadband gateway
- Configure the Packet Data Network Gateway (P-GW) parameters for the broadband gateway
- Configure the APN parameters for the specific APN
- Configure an application identification profile

For information about configuring application profiles, see [Configuring Application Profiles](#) in the Junos OS Application Identification feature documentation.

If the PCEF service interface configured is in the form **amsn**, then per-subscriber load balancing is performed. If the PCEF service interface configured is in the form **msn**, then no load balancing (or redundancy) is performed. In either case, the **interface** statement at the **system** hierarchy level of the P-GW is required for all subscriber-aware services because the subscriber is anchored on the services PIC interface.

To configure an application-aware PCEF service for an APN:

1. Configure a services PIC for the PCEF service.

```
[edit unified-edge gateways ggsn-pgw MBG1 system]
user@host# set service-pics interface ams0
```

2. Configure the PCEF profile by specifying a name for the PCEF profile.

```
[edit services pcef]
user@host# edit profile profile-name
```



**NOTE:** In this release, the PCEF profile is a placeholder profile with no configuration options, but must be created to provide future compatibility for PCEF services.

3. Define a service to use as an application-aware PCEF service.

```
[edit services service-set pcef-service-1]
user@host# set tcp-mss 1300
user@host# set service-set-options subscriber-awareness
user@host# set pcef-profile profile-name
user@host# set application-identification app-id-profile-name
user@host# set interface-service service-interface ams0
```

4. Apply the PCEF application-aware service to the mobile interface for the APN for both ingress and egress traffic so that all traffic arriving on the APN is inspected for application-based charging and policy.

```
[edit interfaces mif unit 0 family inet service]
user@host# set input service-set pcef-service-1
user@host# set output service-set pcef-service-1
```

5. Configure a Deep Packet Inspection (DPI) filter for application-aware traffic.

```
user@host# edit firewall family inet service-filter dpi-filter-1
user@host# set term dpi-flow from redirect-reason dpi
```

```
user@host# set term dpi-flow then service
```

6. Apply the DPI filter so that only application-aware traffic is forwarded to the services PIC.

```
[edit interfaces mif unit 5]
user@host# set clear-dont-fragment-bit
user@host# set family inet service input service-set dpi-service service-filter dpi-filter-1
user@host# set family inet service output service-set dpi-service service-filter dpi-filter-1
```

7. Include the `jservice-appid`, `jservice-pcef`, and `jservice-mss` packages with the services PIC configuration.

```
[edit chassis fpc 3 pic 0 adaptive-services service-package extension-provider]
user@host# set package jservices-appid
user@host# set package jservices-mss
user@host# set package jservices-pcef
```

#### Related Documentation

- [Configuring Application-Aware Policy and Charging Control Rules on page 371](#)
- [Application-Aware Policy and Charging Control Rules Overview on page 353](#)

## Configuring Service Data Flow Filters (Flow Identifiers)

A service data flow (SDF) filter configured at `[edit unified-edge pcef flow-descriptions flow-identifier]` hierarchy level specifies one or more IP packet parameters (source IP, destination IP, source port, destination port, and protocol type) that the policy and charging enforcement function (PCEF) uses to detect IP packets that belong to a specific service session. An SDF filter configured as a flow identifier comprises all the IP packets that match the SDF filter.

A service data flow filter is specified in the **from** clause of a Policy and Charging Control (PCC) rules configuration.



**NOTE:** If you configure a flow identifier SDF for a remote-address, port, port-range, or protocol without specifying a corresponding value, then any value for the SDF filter type is accepted.

To configure Layer 3 and Layer 4 SDF filters:

1. Specify a name for the flow identifier that you want to configure to detect IP packets for a service data flow.

```
[edit unified-edge pcef]
user@host# set flow-descriptions flow-identifier
```

2. Specify the flow direction for the SDF filter.

```
[edit unified-edge pcef flow-descriptions flow-identifier]
user@host# set direction (uplink | downlink | both)
```

3. Specify an IPv4 subnet for the SDF filter.

```
[edit unified-edge pcef flow-descriptions flow-identifier]
```

```
user@host# set remote-address ipv4-address 10.11.12.14/32
```

4. Specify an IPv6 subnet for the SDF filter.

```
[edit unified-edge pcef flow-descriptions flow-identifier]  
user@host# set remote-address ipv6-address 2000.1.2.3::1/128
```

5. Specify a protocol (by number) for the SDF filter.

```
[edit unified-edge pcef flow-descriptions flow-identifier]  
user@host# set protocol 17
```

6. Specify a local port for the SDF filter.

```
edit unified-edge pcef flow-descriptions flow-identifier  
user@host# set local-ports 110
```



**NOTE:** You can configure a local port or local port range but not both in the same SDF filter.

7. Specify from one to three remote ports for the SDF filter.

```
[edit unified-edge pcef flow-descriptions flow-identifier]  
user@host# set remote-ports 999
```



**NOTE:** You can configure a remote port or remote port range but not both in the same SDF filter.

8. Specify a local port range for the SDF filter.

```
[edit unified-edge pcef flow-descriptions flow-identifier]  
user@host# set local-ports low 20 high 100
```

9. Specify a remote port range for the SDF filter.

```
[edit unified-edge pcef flow-descriptions flow-identifier]  
user@host# set remote-ports low 20 high 100
```

10. Specify that signaling information about the SDF filter is not sent to the user equipment (UE), for example, when an SDF filter is applied in the downlink direction only.

```
[edit unified-edge pcef flow-descriptions flow-identifier]  
user@host# set no-send-ue
```

**Related Documentation**

- [Policy and Charging Control Rules Overview on page 349](#)

## Configuring Policy and Charging Control Action Profiles

A Policy and Charging Control (PCC) action profile defines the quality-of-service (QoS) treatment and charging treatment to apply to a service data flow. A PCC action profile is specified in the **then** clause of a PCC rule.

To configure PCC action profiles:

1. Specify a name for the PCC action profile.

```
[edit unified-edge pcef]
user@host# edit pcc-action-profiles profile-name
```

2. Configure the QoS Class Identifier (QCI) by entering a QCI value from 1 through 9.

```
[edit unified-edge pcef pcc-action-profiles profile-name]
user@host# set qci n
```

3. Configure the allocation and retention priority level by entering a priority level from 1 through 15.

```
[edit unified-edge pcef pcc-action-profiles profile-name allocation-retention-priority]
user@host# set priority-level n
```

4. Configure the preemption capability.

```
[edit unified-edge pcef pcc-action-profiles profile-name allocation-retention-priority]
user@host# set preemption-capability (enable | disable)
```

5. Configure the preemption vulnerability.

```
[edit unified-edge pcef pcc-action-profiles profile-name allocation-retention-priority]
user@host# set preemption-vulnerability (enable | disable)
```

6. Configure the maximum bit-rate for uplink and downlink subscriber traffic.

```
[edit unified-edge pcef pcc-action-profiles profile-name]
user@host# set maximum-bit-rate uplink n downlink n
```

7. Configure the guaranteed bit-rate values for uplink and downlink subscriber traffic.

```
[edit unified-edge pcef pcc-action-profiles profile-name]
user@host# set guaranteed-bit-rate uplink n downlink n
```



**NOTE:** Guaranteed bit-rate values are only valid for GTP version 2 and GTP version 1 Release 9.

8. Configure the gating status by enabling or disabling the forwarding of service flow packets.

```
[edit unified-edge pcef pcc-action-profiles profile-name]
user@host# set gate-status (uplink | downlink | uplink-downlink | disable-both)
```

9. Configure the rating-group number for charging.

```
[edit unified-edge pcef pcc-action-profiles profile-name charging]
user@host# set rating-group n
```

10. Configure the service identifier number for online charging.

```
[edit unified-edge pcef pcc-action-profiles profile-name charging]
user@host# set service-identifier n
```

11. Configure the charging method.

```
[edit unified-edge pcef pcc-action-profiles profile-name charging]
user@host# set charging-method (online | offline | online-offline | none)
```



**NOTE:** If a charging-method is not configured, the bearer-level charging method applies. If the charging-method is configured with none, then no charging is applied for the PCC rules.

12. Configure the measurement method for charging.

```
[edit unified-edge pcef pcc-action-profiles profile-name charging]
user@host# set measurement-method (volume | time | volume-time)
```

13. Specify the application-function charging identifier for enabling charging correlation between the application and bearer layer, if the application layer has provided this information via the Rx interface.

```
[edit unified-edge pcef pcc-action-profiles profile-name charging
  application-function-record-info]
user@host# set af-charging-identifier identifier
```

14. Enable service-ID level reporting.

```
[edit unified-edge pcef pcc-action-profiles profile-name charging]
user@host# set service-id-level-reporting
```

**Related  
Documentation**

- [Policy and Charging Control Rules Overview on page 349](#)
  - [Understanding How Dynamic and Static Policy and Charging Control Rules Are Provisioned on page 359](#)
- pcc-action-profiles*
- *charging*

---

## Configuring Layer 3 and Layer 4 Policy and Charging Control Rules

Before you configure Policy and Charging Control (PCC) rules for Layer 3 and Layer 4 traffic, you must do the following:

- Configure the flow identifiers that the PCC rules reference.
- Configure the PCC action profiles that the PCC rules reference.

To configure Layer 3 and Layer 4 PCC rules:

1. Specify a name for the PCC rules.

```
[edit unified-edge pcef]
user@host# edit pcc-rules pcc-rule-name1
```



- Specify one or more flow identifiers that define the Layer 3 and Layer 4 match conditions for filtering subscriber traffic.

```
[edit unified-edge pcef pcc-rules pcc-rule-name1]
user@host# set from flows flow-identifier1
user@host# set from flows flow-identifier2
user@host# set from flows flow-identifier3
```

- Specify the PCC rules action profile that defines the quality of service (QoS), charging, and gating controls for the service data flow.

```
[edit unified-edge pcef pcc-rules pcc-rule-name1]
user@host# set then pcc-action-profile action-profile-name1
```

#### Related Documentation

- [Policy and Charging Enforcement Function Overview on page 347](#)
- [Application-Aware Policy and Charging Control Rules Overview on page 353](#)
- [Configuring a Policy and Charging Control Rulebase on page 372](#)
- [Configuring Application-Aware Policy and Charging Control Rules on page 371](#)

## Configuring Application-Aware Policy and Charging Control Rules

Before you configure application-aware Policy and Charging Control (PCC) rules, you must do the following:

- Configure the flow identifiers that the PCC rules reference.
- Configure the applications, application groups, and nested applications (not already included as predefined application signatures in the Junos OS) that you want to reference in application-aware PCC rules. You use the application identification feature to configure application signatures.
- Configure the PCC action profiles that the PCC rules reference.



**NOTE:** When specifying application-aware PCC rules in a PCEF profile, you must also configure a default Layer 3 or Layer 4 wildcard PCC rule to ensure that the default charging characteristics are applied to unmatched subscriber traffic without dropping that traffic. For example, the default Layer 3 or Layer 4 wildcard PCC rule prevents traffic based on DNS queries from being dropped. In addition, the policy (PCEF profile) that includes application-aware PCC rules must also include a wildcard Layer 3 or Layer 4 PCC rule at a lower precedence.

To configure application-aware PCC rules:

- Specify a name for the PCC rules.

```
[edit unified-edge pcef ]
user@host# edit pcc-rules pcc-rule-name1
```

2. In a **from** statement, specify a flow identifier to use Layer 3 or Layer 4 match conditions for filtering subscriber traffic.

```
[edit unified-edge pcef pcc-rules pcc-rule-name1]  
user@host# set from flows flow-identifier1
```

3. Specify an application (defined in the application identification configuration) as a match condition for filtering subscriber traffic.

```
[edit unified-edge pcef pcc-rules pcc-rule-1]  
user@host# set from applications app-1
```

4. Group multiple applications instead of specifying each application separately, by specifying an application group (defined in the application identification configuration) as a match condition for filtering subscriber traffic.

```
[edit unified-edge pcef pcc-rules pcc-rule-1]  
user@host# set from application-groups app-group-name-1
```

5. Specify a nested application (defined in a Junos configuration) as a match condition for filtering subscriber traffic.

```
[edit unified-edge pcef pcc-rules pcc-rule-1]  
user@host# set from nested-applications nest-app-1
```

6. Specify the PCC rules action profile that defines the quality of service (QoS), charging, and gating controls for the application-level SDF filters.

```
[edit unified-edge pcef pcc-rules pcc-rule-1]  
user@host# set then pcc-action-profile action-profile-1
```

**Related  
Documentation**

- [Application-Aware Policy and Charging Control Rules Overview on page 353](#)
- [Configuring Policy and Charging Enforcement Function Services for Application-Aware Traffic on page 365](#)
- [Configuring a Policy and Charging Control Rulebase on page 372](#)

---

## Configuring a Policy and Charging Control Rulebase

A Policy and Charging Control (PCC) rulebase contains a set of PCC rules. Each rule specified in the PCC rulebase is assigned a precedence to designate the priority in which PCC rules are evaluated for selection in a policy and charging enforcement function (PCEF) profile.

Before you configure a PCC rulebase, you must do the following:

- Configure service data flow filters.
- Configure PCC action profiles.
- Configure PCC rules.

To configure a PCC rulebase:

1. Specify a name for the rulebase.

```
[edit unified-edge pcef]
user@host# edit pcc-rulebases rulebase-name
```

- Specify the PCC rules that the rulebase references and a precedence value (1 through 65,535) for each rule.

```
[edit unified-edge pcef pcc-rulebases rulebase-name]
user@host# set pcc-rule rule-name1 precedence 10
user@host# set pcc-rule rule-name2 precedence 11
user@host# set pcc-rule rule-name3 precedence 12
```

**NOTE:**

- The same rule can be configured in different rulebases and can have a different precedence.
- The precedence assigned must be unique among the configured PCC rules.
- The higher the precedence value the lower the precedence and vice-versa; for example, if a PCC rulebase has two PCC rules with precedence 5 and 10 respectively, the PCC rule with precedence 5 is evaluated first and then the PCC rule with precedence 10 is evaluated.

**Related Documentation**

- [Policy and Charging Enforcement Function Overview on page 347](#)
- [Configuring Layer 3 and Layer 4 Policy and Charging Control Rules on page 370](#)
- *pcc-rulebases (PCEF)*
- *pcc-rules (PCEF)*

## Configuring Event Trigger Profiles

Event triggers are configured on the policy and charging enforcement function (PCEF) to notify the Policy and Charging Rule Function (PCRF) about changes in the access network. An event trigger profile contains one or more event triggers and can be referenced in a PCEF profile configured with dynamic policy control. The PCRF is notified by the PCEF about the event triggers that are configured in an event trigger profile.

To configure an event trigger profile:

- Specify a name for the event trigger profile.

```
[edit unified-edge pcef]
user@host# edit pcef event-trigger-profiles event-trigger-name
```

- Configure an event trigger to send notification to the PCRF when the broadband gateway or PCEF detects a change in the IP-CAN type.

```
[edit unified-edge pcef event-trigger-profiles event-trigger-name]
user@host# set ip-can-change
```

- Configure an event trigger to send notification to the PCRF when the broadband gateway detects a Traffic Flow Template (TFT) change at the bearer level.

```
[edit unified-edge pcef event-trigger-profiles event-trigger-name]  
user@host# set tft-change
```

4. Configure an event trigger to send notification to the PCRF when the broadband gateway detects a Public Land Mobile Network (PLMN) change.

```
[edit unified-edge pcef event-trigger-profiles event-trigger-name]  
user@host# set plmn-change
```

5. Configure an event trigger to send notification to the PCRF when the broadband gateway detects a change in the Routing Area Identity (RAI) of the Serving Gateway (S-GW) or Serving GPRS Support Node (SGSN) where the user equipment (UE) is registered.

```
[edit unified-edge pcef event-trigger-profiles event-trigger-name]  
user@host# set rai-change
```

6. Configure an event trigger to send notification to the PCRF when the broadband gateway detects a change in the Radio Access Technology (RAT) that is serving the user equipment.

```
[edit unified-edge pcef event-trigger-profiles event-trigger-name]  
user@host# set rat-change
```

7. Configure an event trigger to send notification to the PCRF when the broadband gateway detects that the user equipment has moved to a new S-GW or SGSN.

```
[edit unified-edge pcef event-trigger-profiles event-trigger-name]  
user@host# set sgsn-change
```

8. Configure an event trigger to send notification to the PCRF when the broadband gateway detects that the time zone in which the user equipment is located has changed.

```
[edit unified-edge pcef event-trigger-profiles event-trigger-name]  
user@host# set ue-timezone-change
```

9. Configure an event trigger to send notification to the PCRF when the broadband gateway detects a change in the user location.

```
[edit unified-edge pcef event-trigger-profiles event-trigger-name]  
user@host# set user-location-change
```

**Related  
Documentation**

- [Understanding Event Triggers on page 363](#)
- [event-trigger-profiles](#)

## Configuring a Policy and Charging Enforcement Function Profile for Dynamic Policies

When a policy and charging enforcement function (PCEF) profile is configured with dynamic policy control, the policy and charging rules function (PCRF) can provision both Policy and Charging Control (PCC) rules and PCC rule names over the Gx interface.

Before you configure a PCEF profile for dynamic policies, you must do the following:

- Configure a Diameter Gx profile.
- Configure service data flow (SDF) filters (optional).
- Configure a PCC action profile (optional).
- Configure PCC rules, PCC rulebases, or both (optional).
- Configure an event trigger profile (optional).



**NOTE:** When a PCEF profile includes application-aware PCC rules, you must also include a default Layer3 or Layer4 wildcard PCC rule to ensure that the default charging characteristics are applied to unmatched subscriber traffic without dropping that traffic. For example, the default Layer 3 or Layer 4 wildcard PCC rule prevents traffic based on DNS queries from being dropped. In addition, the PCEF profile that includes application-aware PCC rules must also include a wildcard Layer 3 or Layer 4 PCC rule at a lower precedence.

1. To configure a PCEF profile, specify a name for the PCEF profile for dynamic policies.

```
[edit unified-edge pcef]
```

```
user@host# edit profiles pcef-dynamic-services-profile-name
```

2. Specify one or more PCC rules and a precedence for each rule.

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile-name]
```

```
user@host# set dynamic-policy-control pcc-rules pcc-rule-name1 precedence 5
```

```
user@host# set dynamic-policy-control pcc-rules pcc-rule-name2 precedence 6
```

```
user@host# set dynamic-policy-control pcc-rules pcc-rule-name3 precedence 7
```

You can assign a precedence value from 1 through 65,535.



**NOTE:**

- The precedence assigned must be unique among the configured PCC rules.
- The higher the precedence value the lower the precedence and vice-versa; for example, if a PCC profile has two PCC rules with precedence 5 and 10 respectively, the PCC rule with precedence 5 is evaluated first and then the PCC rule with precedence 10 is evaluated.

3. Specify one or more PCC rulebases.

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile-name]
```

```
user@host# set dynamic-policy-control pcc-rulebases rulebase-name1
user@host# set dynamic-policy-control pcc-rulebases rulebase-name2
```



**NOTE:** The PCC rules and PCC rulebases configured in a PCEF profile should not overlap.

4. Specify the action to be initiated when the PCRF goes down.

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile-name
dynamic-policy-control failure-handling]
user@host# edit failure-action (continue | continue-and-retry | terminate)
```

5. If the **edit failure-action terminate** action is configured in the PCEF profile, specify the name of the PCC rule or PCC rulebase to apply to start a new session after the existing session terminates.

- To specify a PCC rule to apply to start a new session:

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile-name
dynamic-policy-control failure-handling]
user@host# set pcc-rules rule-name1 precedence 5
```

- To specify a PCC rulebase to apply to start a new session:

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile-name
dynamic-policy-control failure-handling]
user@host# set pcc-rulebases rulebase-name1
```

6. Specify a Diameter Gx profile.

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile-name
dynamic-policy-control]
user@host# edit diameter-profile diameter-profile-name
```

7. Specify the release that the Gx interface uses at the PDN gateway (P-GW) so that the P-GW receives only the AVPs compliant to the release version configured.

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile-name
dynamic-policy-control]
user@host# set release (rel8 | rel9)
```

8. Specify that online charging sessions should not fail over to an alternate server.

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile-name
dynamic-policy-control]
user@host# edit session-failover-not-supported
```

#### Related Documentation

- [Configuring APN Service Selection on a Broadband Gateway on page 135](#)
- [Configuring a Policy and Charging Enforcement Function Profile for Static Policies on page 377](#)
- [Configuring a Policy and Charging Control Rulebase on page 372](#)
- [dynamic-policy-control](#)
- [pcef](#)
- [Policy and Charging Control Rules Overview on page 349](#)

- [Policy and Charging Enforcement Function Overview on page 347](#)

## Configuring a Policy and Charging Enforcement Function Profile for Static Policies

A policy and charging enforcement function (PCEF) profile configured for static policy control specifies that Policy and Charging Control (PCC) rules are provisioned by the PCEF with no interaction from the policy and charging rules function (PCRF) and no Gx interface support.

Before you configure a PCEF profile for static policies, you must do the following:

- Configure service data flow filters for PCC rules.
- Configure PCC action profiles for PCC rules.
- Configure PCC rules.
- Configure PCC rulebases (optional).

To configure a PCEF profile:

1. Specify a name for the PCEF profile for static policies.

```
[edit unified-edge pcef]
user@host# edit profile pcef-static-services-profile-name
```

2. Specify one or more PCC rules and a precedence for each rule.

```
[edit unified-edge pcef profiles pcef-static-services-profile-name static-policy-control]
user@host# set pcc-rules rule-name1 precedence 10
user@host# set pcc-rules rule-name2 precedence 11
user@host# set pcc-rules rule-name3 precedence 12
```

You can assign a precedence value from 1 through 65,535.



### NOTE:

- The precedence assigned must be unique among the configured PCC rules.
- The higher the precedence value the lower the precedence and vice-versa; for example, if a PCC profile has two PCC rules with precedence 5 and 10 respectively, the PCC rule with precedence 5 is evaluated first and then the PCC rule with precedence 10 is evaluated.

3. Specify one or more PCC rule bases.

```
[edit unified-edge pcef profiles pcef-static-services-profile-name static-policy-control]
user@host# set pcc-rulebases rulebase-name1
user@host# set pcc-rulebases rulebase-name2
```

4. Specify that a Create Session request creates a dedicated bearer with the specified QCI value, in addition to the default bearer.

```
[set unified-edge pcef profiles pcef-static-services-profile-name static-policy-control]
user@host# set activate-dedicated-bearers 5
```



**NOTE:** A dedicated bearer can be associated with any QoS Class Identifier (QCI) value (1 through 9). For each QCI value you configure with the `activate-dedicated-bearers` statement, a separate dedicated bearer is created.

#### Related Documentation

- [Configuring APN Service Selection on a Broadband Gateway on page 135](#)
- [Configuring a Policy and Charging Control Rulebase on page 372](#)
- [Configuring a Policy and Charging Enforcement Function Profile for Dynamic Policies on page 375](#)
- *pcef*
- [Policy and Charging Control Rules Overview on page 349](#)
- [Policy and Charging Enforcement Function Overview on page 347](#)
- *static-policy-control*

## Tracing PCEF Operations

To configure tracing operations for the policy and charging enforcement function (PCEF):

1. Specify that you want to configure tracing options for PCEF.  

```
[edit unified-edge pcef]
user@host# edit traceoptions
```
2. (Optional) Configure the name of the file used for the trace output.  

```
[edit unified-edge pcef]
user@host# set file filename
```
3. (Optional) Configure flags to filter the operations to be logged.  

```
[edit unified-edge pcef]
user@host# set flag flag
```

| Flag              | Description                                                 |
|-------------------|-------------------------------------------------------------|
| all               | Trace all operations                                        |
| config            | Trace configuration events                                  |
| debug             | Trace the debug internal events                             |
| fsm               | Trace FSM                                                   |
| general           | Trace general events that do not fit in any specific traces |
| high-availability | Trace high availability events                              |



| Flag   | Description                 |
|--------|-----------------------------|
| init   | Trace initialization events |
| tftmgr | Trace tftmgr events         |

4. (Optional) Configure the level of tracing.

```
[edit unified-edge pcef]
user@host# set level (all | critical | error | info | notice | verbose | warning)
```

**Related Documentation**

- [traceoptions \(PCEF\)](#)

## Example: Configuring Policy and Charging Enforcement Function With Layer 3 and Layer 4 Policy and Charging Control Rules

This example shows how to configure the policy and charging enforcement function (PCEF) on the MobileNext Broadband Gateway. The PCEF manages user-plane traffic handling control on the Gateway GPRS Support Node (GGSN) or Packet Data Network Gateway (P-GW) by providing service data flow detection, quality-of-service (QoS) control, charging control, and gating status.

- [Requirements on page 379](#)
- [Overview on page 380](#)
- [Configuration on page 381](#)
- [Verification on page 390](#)
- [Troubleshooting on page 395](#)

### Requirements

This example uses the following hardware and software components:

- A supported MX Series chassis configured with supported line cards and a services PIC.
- A supported and properly installed version of 64-bit Junos OS and the **jmobile** software package.
- Correct configuration as a P-GW with corresponding interfaces.

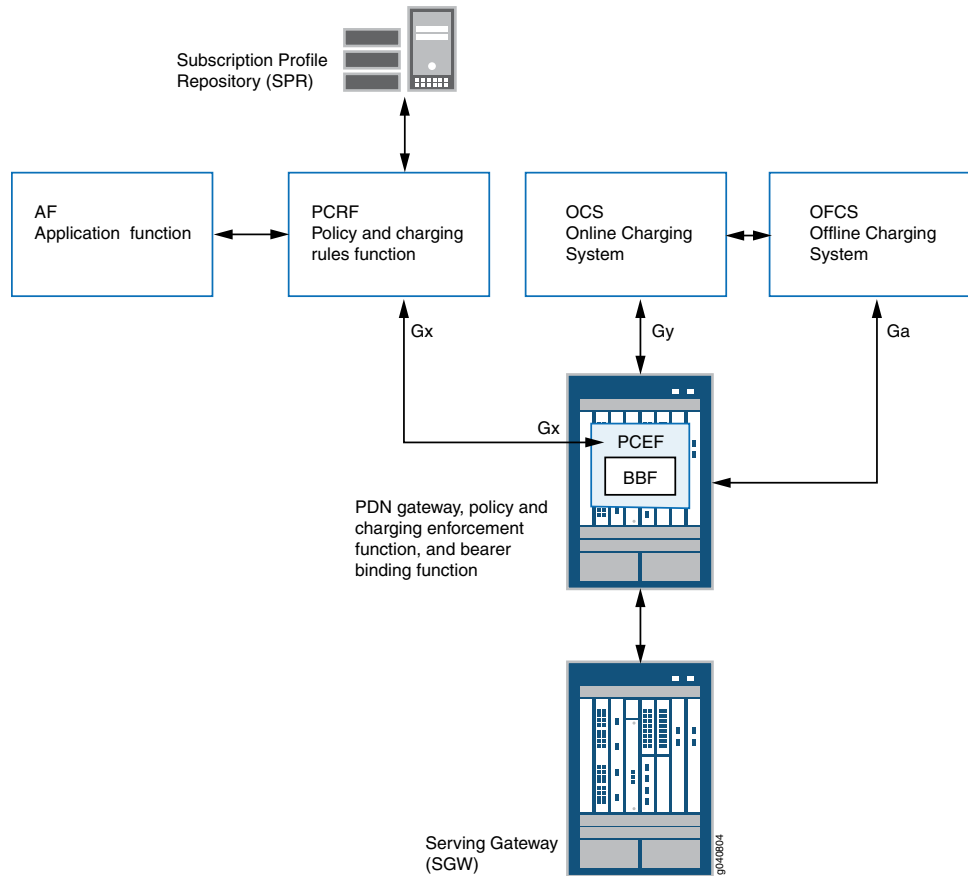
Before you begin:

- Configure GTP and Diameter.
- Configure mobile interfaces for access point names (APNs).
- Configure APNs.
- Configure the policy and charging rule function (PCRF).

## Overview

The PCEF is part of a complete broadband gateway configuration, including online and offline charging, and quality-of-service (QoS) determination. [Figure 51 on page 380](#) shows the overall architecture for the gateway components and the functional groupings for policy and charging. The Gx interface connects the PCEF and the PCRF.

**Figure 51: Architecture for Policy and Charging Enforcement Function**



## Topology

The topology for this PCEF example consists of mobile network nodes and the interfaces connecting them. The key component is the PCEF, which enforces policy decisions that are received from the PCRF and provides the PCRF with user and access information over the Gx reference point. The PCEF also interacts with the Online Charging System (OCS), which provides credit management for prepaid charging, and reports resource usage to the Offline Charging System (OFCS).

## Configuration

To configure the PCEF on the P-GW, perform these tasks:

- [Configuring Service Data Flow Filters on page 381](#)
- [Configuring PCC Action Profiles on page 382](#)
- [Configuring PCC Rules on page 384](#)
- [Configuring a PCC Rulebase on page 386](#)
- [Configuring an Event Trigger Profile on page 386](#)
- [Configuring a Diameter Gx Profile for Dynamic Services on page 387](#)
- [Configuring a PCEF Profile for Dynamic Services on page 387](#)
- [Configuring a PCEF Profile for Static Services on page 388](#)
- [Applying a PCEF Policy for Dynamic Services to an APN on page 389](#)
- [Applying a PCEF Profile for Static Services to an APN on page 389](#)
- [Results on page 390](#)

### Configuring Service Data Flow Filters

#### CLI Quick Configuration

To quickly configure the service data flow filters, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge pcef flow-descriptions application-flow-1]
set direction both
set remote-ports 80
[edit unified-edge pcef flow-descriptions application2-flow-1]
set direction both
set remote-address ipv4-address 15.16.17.0/24
[edit unified-edge pcef flow-descriptions dns-flow-1]
set direction both
set remote-address ipv4-address 10.11.12.14/32
[edit unified-edge pcef flow-descriptions dns-flow-2]
set direction both
set remote-address ipv4-address 10.11.12.24/32
[edit unified-edge pcef flow-descriptions ipv6-gaming-flow]
set direction both
set remote-address remote-address ipv6-address 2000:1:2:3::1/128
[edit unified-edge pcef flow-descriptions sip-server-flow-1]
set remote-port-range low 5000 high 6000
set remote-address ipv4-address 12.13.14.16/32
[edit unified-edge pcef flow-descriptions video-svc-flow-1]
set direction both
set remote-address ipv4-address 11.12.13.14/32
[edit unified-edge pcef flow-descriptions video-svc-flow-2]
set direction both
set remote-address ipv4-address 11.12.13.15/32
```

#### Step-by-Step Procedure

To configure the service data flow filters:

1. Configure service data flow filters for HTTP traffic.

```
[edit]
user@host# set unified-edge pcef flow-descriptions application-flow-1 direction
both remote-ports 80
user@host# set unified-edge pcef flow-descriptions application2-flow-1 direction
both remote-address ipv4-address 15.16.17.0/24
```

2. Configure service data flow filters for traffic going to Domain Name System (DNS) servers. For example, ensure that any mobile traffic going to the operator's own infrastructure (in this case, a DNS server) is not charged.

```
[edit]
user@host# set unified-edge pcef flow-descriptions dns-flow-1 direction both
remote-address ipv4-address 10.11.12.14/32
user@host# set unified-edge pcef flow-descriptions dns-flow-2 direction both
remote-address ipv4-address 10.11.12.24/32
```

3. Configure service data flow filters for real-time gaming traffic.

```
[edit]
user@host# set unified-edge pcef flow-descriptions ipv6-gaming-flow direction
both remote-address ipv6-address 2000:1:2:3::1/128
```

4. Configure service data flow filters for VoIP traffic.

```
[edit]
user@host# set unified-edge pcef flow-descriptions sip-server-flow-1
remote-port-range low 5000 high 6000
user@host# set unified-edge pcef flow-descriptions sip-server-flow-1 ipv4-address
12.13.14.16/32
```

5. Configure service data flow filters for streaming video traffic.

```
[edit]
user@host# set unified-edge pcef flow-descriptions video-svc-flow-1 direction both
remote-address ipv4-address 11.12.13.14/32
```

6. Configure service data flow filters for interactive video traffic.

```
[edit]
user@host# set unified-edge pcef flow-descriptions video-svc-flow-2 direction
both remote-address ipv4-address 11.12.13.15/32
```

---

### Configuring PCC Action Profiles

**CLI Quick Configuration** To quickly configure the Policy and Charging Control (PCC) action profiles, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge pcef pcc-action-profiles app1-action]
set qci 8
set allocation-retention-priority priority-level 12
set charging rating-group 5
set charging service-identifier 10
set charging charging-method offline
set charging measurement-method volume
[edit unified-edge pcef pcc-action-profiles app2-action]
set qci 8
set allocation-retention-priority priority-level 12
set charging rating-group 20
set charging service-identifier 30
```

```

set charging charging-method offline
set charging measurement-method volume
[edit unified-edge pcef pcc-action-profiles dns-action]
set qci 7
set allocation-retention-priority priority-level 15
set allocation-retention-priority preemption-capability disable
set allocation-retention-priority preemption-vulnerability enable
[edit unified-edge pcef pcc-action-profiles ipv6-gaming-action]
set qci 3
set maximum-bit-rate uplink 3000
set maximum-bit-rate downlink 5000
set charging rating-group 5
set charging charging-method online
set charging measurement-method time
[edit unified-edge pcef pcc-action-profiles sip-signalling-action]
set qci 5
set allocation-retention-priority priority-level 3
[edit unified-edge pcef pcc-action-profiles video-service-action]
set qci 4
set allocation-retention-priority priority-level 8
set maximum-bit-rate uplink 1000
set maximum-bit-rate downlink 10000
set guaranteed-bit-rate uplink 100
set guaranteed-bit-rate downlink 1000

```

#### Step-by-Step Procedure

To configure the PCC action profiles:

1. Configure the PCC action profiles for HTTP traffic.

```

[edit]
user@host# set unified-edge pcef pcc-action-profiles app1-action qci 8
user@host# set unified-edge pcef pcc-action-profiles app1-action
allocation-retention-priority priority-level 12
user@host# set unified-edge pcef pcc-action-profiles app1-action charging
rating-group 5
user@host# set unified-edge pcef pcc-action-profiles app1-action charging
service-identifier 10
user@host# set unified-edge pcef pcc-action-profiles app1-action charging
charging-method offline
user@host# set unified-edge pcef pcc-action-profiles app1-action charging
measurement-method volume
user@host# set unified-edge pcef pcc-action-profiles app2-action qci 8
user@host# set unified-edge pcef pcc-action-profiles app2-action
allocation-retention-priority priority-level 12
user@host# set unified-edge pcef pcc-action-profiles app2-action charging
rating-group 20
user@host# set unified-edge pcef pcc-action-profiles app2-action charging
service-identifier 30
user@host# set unified-edge pcef pcc-action-profiles app2-action charging
charging-method offline
user@host# set unified-edge pcef pcc-action-profiles app2-action charging
measurement-method volume

```

2. Configure a PCC action profile for traffic directed to Domain Name System (DNS) servers. For example, ensure that any mobile traffic going to the operator's own infrastructure (in this case, a DNS server) is not charged.

```
[edit]
user@host# set unified-edge pcef pcc-action-profiles dns-action qci 7
user@host# set unified-edge pcef pcc-action-profiles dns-action
  allocation-retention-priority priority-level 15
user@host# set unified-edge pcef pcc-action-profiles dns-action
  allocation-retention-priority preemption-capability disable
user@host# set unified-edge pcef pcc-action-profiles dns-action
  allocation-retention-priority preemption-vulnerability enable
```

3. Configure a PCC action profile for IPv6 real-time gaming traffic.

```
[edit]
user@host# set unified-edge pcef pcc-action-profiles ipv6-gaming-action qci 3
user@host# set unified-edge pcef pcc-action-profiles ipv6-gaming-action
  maximum-bit-rate uplink 3000
user@host# set unified-edge pcef pcc-action-profiles ipv6-gaming-action
  maximum-bit-rate downlink 5000
user@host# set unified-edge pcef pcc-action-profiles ipv6-gaming-action charging
  rating-group 5
user@host# set unified-edge pcef pcc-action-profiles ipv6-gaming-action charging
  charging-method online
user@host# set unified-edge pcef pcc-action-profiles ipv6-gaming-action charging
  measurement-method time
```

4. Configure a PCC action profile for VoIP traffic.

```
[edit]
user@host# set unified-edge pcef pcc-action-profiles sip-signalling-action qci 5
user@host# set unified-edge pcef pcc-action-profiles sip-signalling-action
  allocation-retention-priority priority-level 3
```

5. Configure a PCC action profile for streaming video and interactive video traffic.

```
[edit]
user@host# set unified-edge pcef pcc-action-profiles video-service-action qci 4
user@host# set unified-edge pcef pcc-action-profiles video-service-action
  allocation-retention-priority priority-level 8
user@host# set unified-edge pcef pcc-action-profiles video-service-action
  maximum-bit-rate uplink 1000
user@host# set unified-edge pcef pcc-action-profiles video-service-action
  maximum-bit-rate downlink 10000
user@host# set unified-edge pcef pcc-action-profiles video-service-action
  guaranteed-bit-rate uplink 100
user@host# set unified-edge pcef pcc-action-profiles video-service-action
  guaranteed-bit-rate downlink 1000
```

---

### Configuring PCC Rules

#### CLI Quick Configuration

To quickly configure PCC rules, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge pcef pcc-rules app1-rule]
set from flows application-flow-1
set then pcc-action-profile app1-action
[edit unified-edge pcef pcc-rules app2-rule]
set from flows application2-flow-1
set then pcc-action-profile app2-action
```

```

[edit unified-edge pcef pcc-rules dns-rule]
set from flows dns-flow-1
set from flows dns-flow-2
set then pcc-action-profile dns-action
[edit unified-edge pcef pcc-rules ipv6-gaming-rule]
set from flows ipv6-gaming-flow
set then pcc-action-profile ipv6-gaming-action
[edit unified-edge pcef pcc-rules sip-signaling-rule]
set from flows sip-signaling-flow
set then pcc-action-profile sip-signaling-action
[edit unified-edge pcef pcc-rules video-service-rule]
set from flows video-svc-flow-1
set from flows video-svc-flow-2
set then pcc-action-profile video-service-action
[edit unified-edge pcef pcc-rulebases app-rule-base]
set pcc-rule app1-rule precedence 510
set pcc-rule app2-rule precedence 520
[edit unified-edge pcef profiles pcef-static-services-profile]
[edit unified-edge pcef profiles pcef-dynamic-services-profile dynamic-policy-control]
set pcc-rules video-service-rule precedence 500
set pcc-rulebases app-rule-base
set diameter-profile gx1
[edit unified-edge pcef profiles pcef-dynamic-services-profile static-policy-control]
set pcc-rules sip-signalling-rule precedence 1000
set activate-dedicated-bearers 5
set pcc-rules ip v6-real-time-gaming precedence 1
set activate-dedicated-bearers 3

```

**Step-by-Step Procedure** To configure PCC rules for the MobileNext Broadband Gateway:

1. Configure PCC rules for HTTP traffic (application 1).
 

```

[edit unified-edge pcef pcc-rules app1-rule]
user@host# set from flows application-flow-1
user@host# set then pcc-action-profile app1-action

```
2. Configure PCC rules for HTTP traffic (application 2).
 

```

[edit unified-edge pcef pcc-rules app2-rule]
user@host# set from flows application2-flow-1
user@host# set then pcc-action-profile app2-action

```
3. Configure PCC rules for Domain Name Server (DNS) traffic.
 

```

[edit unified-edge pcef pcc-rules dns-rule]
user@host# set from flows dns-flow-1
user@host# set from flows dns-flow-2
user@host# set then pcc-action-profile dns-action

```
4. Configure PCC rules for real-time gaming traffic.
 

```

[edit unified-edge pcef pcc-rules ipv6-gaming-rule]
user@host# set from flows ipv6-gaming-flow
user@host# set then pcc-action-profile ipv6-gaming-action

```
5. Configure PCC rules for IMS service (VoIP) traffic.
 

```

[edit unified-edge pcef pcc-rules sip-signaling-rule]
user@host# set from flows sip-signaling-flow

```

```
user@host# set then pcc-action-profile sip-signaling-action
```

6. Configure PCC rules for streaming video and interactive video traffic.

```
[edit unified-edge pcef pcc-rules video-service-rule]
user@host# set from flows video-svc-flow-1
user@host# set from flows video-svc-flow-2
user@host# set then pcc-action-profile video-service-action
```

---

### Configuring a PCC Rulebase

---

**CLI Quick Configuration** To quickly configure a PCC rulebase, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge pcef pcc-rulebases app-rule-base]
set pcc-rule app1-rule precedence 510
set pcc-rule app2-rule precedence 520
```

**Step-by-Step Procedure**

1. To configure a rulebase, specify a name for the rulebase.  

```
[edit]
user@host# edit unified-edge pcef pcc-rulebases app-rule-base
```
2. Specify the PCC rules that the rulebase references and assign a precedence for each rule.

```
[edit unified-edge pcef pcc-rulebases app-rule-base]
user@host# set pcc-rule app1-rule precedence 510
user@host# set pcc-rule app2-rule precedence 520
```



**NOTE:** The higher the precedence value the lower the precedence and vice-versa. In this example, the PCC rule with precedence 510 is evaluated first and then the PCC rule with precedence 520 is evaluated.

---

---

### Configuring an Event Trigger Profile

---

**CLI Quick Configuration** To quickly configure an event trigger profile, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge pcef event-trigger-profiles evt-trigger1]
set rat-change
set sgsn-change
```

**Step-by-Step Procedure**

To configure an event trigger profile to include in a PCEF dynamic services profile:

1. Specify a name for the event-trigger profile.  

```
[edit unified-edge pcef]
user@host# edit event-trigger-profiles evt-trigger1
```
2. Configure an event trigger to send notification to the PCRF when the broadband gateway detects that the air interface, communicated as the Radio Access Technology (RAT) type, has changed.



```
[edit unified-edge pcef]
user@host# set event-trigger-profiles evt-trigger1 rat_change
```

3. Configure an event trigger to send notification to the PCRF when the broadband gateway detects that Serving Gateway Support Node (SGSN) or Serving Gateway (S-GW) has changed.

```
[edit unified-edge pcef]
user@host# set event-trigger-profiles evt-trigger1 sgsn_change
```

### Configuring a Diameter Gx Profile for Dynamic Services

**CLI Quick Configuration** To quickly configure a Gx profile, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge diameter-profiles gx-profile gx1]
set targets pcef-dne1 destination-realm juniper.net
set targets pcef-dne1 priority 1
set targets pcef-dne1 network-element pcrf-dne1
set targets pcef-dne2 destination-realm juniper.net
set targets pcef-dne2 priority 1
set targets pcef-dne2 network-element pcrf-dne2
```

**Step-by-Step Procedure** To configure the Diameter Gx profile named *gx1* for the Gx application:

1. Specify a name for the Gx profile.

```
[edit unified-edge diameter-profiles]
user@host# edit gx-profile gx1
```

2. Configure the target named *pcef-dne1* for the profile and specify its destination realm, priority, and network element.

```
[edit unified-edge diameter-profiles gx-profile gx1]
user@host# set targets pcef-dne1 destination-realm juniper.net
user@host# set targets pcef-dne1 priority 1
user@host# set targets pcef-dne1 network-element pcrf-dne1
```

3. Configure the target named *pcef-dne2* for the profile and specify its destination realm, priority, and network element.

```
[edit unified-edge diameter-profiles gx-profile gx1]
user@host# set targets pcef-dne2 destination-realm juniper.net
user@host# set targets pcef-dne2 priority 1
user@host# set targets pcef-dne2 network-element pcrf-dne2
```

### Configuring a PCEF Profile for Dynamic Services

**CLI Quick Configuration** To quickly configure a policy and charging enforcement function (PCEF) profile for dynamic policies, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile]
set dynamic-policy-control pcc-rules video-service-rule precedence 500
set dynamic-policy-control pcc-rulebases app-rule-base
set dynamic-policy-control event-trigger evt-trigger1
```

```
set dynamic-policy-control diameter-profile gx1
```

**Step-by-Step  
Procedure**

To configure a PCEF profile:

1. Specify a name for the PCEF profile.

```
[edit unified-edge pcef]  
user@host# edit profiles pcef-dynamic-services-profile
```

2. Specify the PCC rules and precedence.

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile]  
user@host# set dynamic-policy-control pcc-rules video-service-rule precedence  
500
```



**NOTE:** The PCRF will evaluate either the PCC rule base or PCC rules, but not both.

3. Specify a PCC rulebase for the PCEF profile.

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile]  
user@host# set dynamic-policy-control pcc-rulebases app-rule-base1
```

4. Specify an event trigger for the PCEF profile.

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile dynamic-policy-control]  
user@host# set event-trigger evt-trigger1
```

5. Specify a diameter Gx profile for the PCEF profile.

```
[edit unified-edge pcef profiles pcef-dynamic-services-profile dynamic-policy-control]  
user@host# edit diameter-profile gx1
```

---

### Configuring a PCEF Profile for Static Services

---

**CLI Quick  
Configuration**

To quickly configure a PCEF profile for static policies, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge pcef profiles pcef-static-services-profile]  
[edit unified-edge pcef profiles pcef-static-services-profile static-policy-control]  
set pcc-rules sip-signalling-rule precedence 1000  
set pcc-rules ipv6-gaming-rule precedence 1  
set activate-dedicated-bearers 5
```

**Step-by-Step  
Procedure**

To configure a PCEF profile:

1. Specify a name for the PCEF profile.

```
[edit unified-edge]  
user@host# edit pcef profile pcef-static-services-profile
```

2. Specify the PCC rules and rule precedence.

```
[edit unified-edge pcef profiles pcef-static-services-profile static-policy-control]  
user@host# set pcc-rules sip-signaling-rule precedence 1000  
user@host# set pcc-rules ip-v6-real-time-gaming precedence 1
```

- Specify that a Create Session request creates a dedicated bearer, in addition to the default bearer.

```
[edit unified-edge pcef profiles pcef-static-services-profile static-policy-control]
user@host# set activate-dedicated-bearers 5
```

### Applying a PCEF Policy for Dynamic Services to an APN

#### CLI Quick Configuration

To quickly apply the PCEF profile to an access point name (APN), copy the following commands and paste them into the router terminal window:

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns pcef-dynamic-services-apn]
set mobile-interface mif.1
set address-assignment local
set selection-mode from-ms
set pcef-profile pcef-dynamic-services-profile
```

#### Step-by-Step Procedure

To apply a PCEF policy:

- Configure an APN named `pcef-dynamic-services-apn` to use for the `mif.1` interface.

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns
pcef-dynamic-services-apn]
user@host# set mobile-interface mif.1
```

- Configure a `local` address assignment that uses the default mobile pool to assign the IP address. The default pool is configured in the routing instance that is associated with the mobile interface of the APN.

```
[unified-edge gateways ggsn-pgw PGW apn-services apns
pcef-dynamic-services-apn]
user@host# set address-assignment local
```

- Configure the APN to allow a Create Session Request or Create Packet Data Protocol (PDP) Context message with the selection mode IE value of 1.

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns
pcef-dynamic-services-apn]
user@host# set selection-mode from-ms
```

- Configure the APN to use a PCEF dynamic policy to use real-time analysis of the service to assign PCC rules.

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns
pcef-dynamic-services-apn]
user@host# set pcef-profile pcef-dynamic-services-profile
```

### Applying a PCEF Profile for Static Services to an APN

#### CLI Quick Configuration

To quickly apply the PCEF profile to an APN, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns pcef-static-services-apn]
mobile-interface mif.2
set mobile-interface mif.2
set address-assignment local
set selection-mode from-ms
```

```
set pcef-profile pcef-static-services-profile
```

**Step-by-Step  
Procedure**

To apply a PCEF policy:

1. Configure an APN named `pcef-static-services-apn` to use for the `mif.2` interface.  

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns  
pcef-static-services-apn]  
user@host# set mobile-interface mif.2
```
2. Configure a **local** address assignment that uses the default mobile pool to assign the IP address. The default pool is configured in the routing instance that is associated with the mobile interface of the APN.  

```
[unified-edge gateways ggsn-pgw PGW apn-services apns pcef-static-services-apn]  
user@host# set address-assignment local
```
3. Configure the APN to allow a Create Session Request or Create Packet Data Protocol (PDP) Context message with the selection mode IE value of 1.  

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns  
pcef-static-services-apn]  
user@host# set selection-mode from-ms
```
4. Configure the APN to use a PCEF static policy to assign PCC rules.  

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns  
pcef-static-services-apn]  
user@host# set pcef-profile pcef-static-services-profile
```

---

**Results**

From configuration mode, confirm your configuration by entering the **show** command at the correct hierarchy level. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, this **show** command output includes only the configuration that is relevant to this example.

```
[edit unified-edge gateways ggsn-pgw mbg-1 pcef]
```

**Verification**

To display Gx statistics and active bearer statistics to verify the PCEF configuration on the broadband gateway is working properly, you can perform the following tasks:

- [Verifying Control Plane Gx Statistics on the Gateway on page 390](#)
- [Verifying Active Bearers on the Gateway on page 391](#)
- [Verifying Control Plane Gx Statistics on the Gateway on page 392](#)
- [Verifying Control Plane GX Statistics on the APN on page 392](#)

---

**Verifying Control Plane Gx Statistics on the Gateway**

**Purpose** Verify the control plane statistics for the Gx interface on the P-GW.

**Action** user@host> show unified-edge ggsn-pgw statistics

Gateway: PGW

Control plane GTP statistics:

|                                             |   |
|---------------------------------------------|---|
| Session establishment attempts:             | 6 |
| Successful session establishments:          | 6 |
| MS/peer initiated session deactivations:    | 4 |
| Successful MS/peer initiated deactivations: | 4 |
| Gateway initiated session deactivations:    | 0 |
| Successful gateway initiated deactivations: | 0 |

PCC Gx statistics:

|                                              |   |            |
|----------------------------------------------|---|------------|
| Session attempts using dynamic policy:       | 6 | Success: 6 |
| Dedicated bearer activation attempts:        | 5 | Success: 3 |
| MS-Peer init dedicated bearer deactivations: | 2 |            |
| Gateway init dedicated bearer deactivations: | 0 |            |
| PCRF init dedicated bearer deactivations:    | 0 |            |

Data plane global statistics:

|                                   |   |
|-----------------------------------|---|
| Source address violation packets: | 0 |
| Non-existent TEID/TID packets:    | 0 |
| GTP length error packets:         | 0 |
| Non-existent UE address packets:  | 0 |
| Mobile-to-mobile packets:         | 0 |

Data plane GTP statistics (Gn/S5/S8):

|                    |      |
|--------------------|------|
| Input packets:     | 15   |
| Input bytes:       | 1500 |
| Output packets:    | 15   |
| Output bytes:      | 1500 |
| Discarded packets: | 0    |

Data plane GTP statistics (Gi):

|                    |      |
|--------------------|------|
| Input packets:     | 15   |
| Input bytes:       | 1500 |
| Output packets:    | 15   |
| Output bytes:      | 1500 |
| Discarded packets: | 0    |

**Meaning** The **show unified-edge ggsn-pgw statistics** command displays all statistics at the gateway level for different interfaces.

### Verifying Active Bearers on the Gateway

**Purpose** Verify the active bearers on the P-GW.

**Action** user@host> show unified-edge ggsn-pgw status

Gateway: PGW

Mobile gateway status:

|                         |   |    |
|-------------------------|---|----|
| Active Subscribers      | : | 2  |
| Active Sessions         | : | 2  |
| Active Bearers          | : | 3  |
| Active GBR Bearers      | : | 1  |
| Active Non-GBR Bearers  | : | 2  |
| Active Prepaid bearers  | : | 0  |
| Active Postpaid bearers | : | 0  |
| CPU Load (%)            | : | 0  |
| Memory Load (%)         | : | 32 |

**Meaning** The **show unified-edge ggsn-pgw status** command displays the active subscribers, sessions, and bearers on the network.

### Verifying Control Plane Gx Statistics on the Gateway

---

**Purpose** Verify the control plane Gx statistics on the P-GW.

**Action**

```
user@host> show unified-edge ggsn-pgw statistics gateway PGW
Gateway: PGW
Control plane GTP statistics:
  Session establishment attempts:      6
  Successful session establishments:    6
  MS/peer initiated session deactivations: 4
  Successful MS/peer initiated deactivations: 4
  Gateway initiated session deactivations: 0
  Successful gateway initiated deactivations: 0
PCC Gx statistics:
  Session attempts using dynamic policy: 6      Success: 6
  Dedicated bearer activation attempts: 5      Success: 3
  MS-Peer init dedicated bearer deactivations: 2
  Gateway init dedicated bearer deactivations: 0
  PCRF init dedicated bearer deactivations: 0
Data plane global statistics:
  Source address violation packets:      0
  Non-existent TEID/TID packets:        0
  GTP length error packets:             0
  Non-existent UE address packets:      0
  Mobile-to-mobile packets:             0
Data plane GTP statistics (Gn/S5/S8):
  Input packets:                        15
  Input bytes:                         1500
  Output packets:                      15
  Output bytes:                       1500
  Discarded packets:                   0
Data plane GTP statistics (Gi):
  Input packets:                        15
  Input bytes:                         1500
  Output packets:                      15
  Output bytes:                       1500
  Discarded packets:                   0
```

**Meaning** The `show unified-edge ggsn-pgw statistics gateway PGW` command displays gateway-level statistics.

### Verifying Control Plane GX Statistics on the APN

---

**Purpose** Verify the control plane statistics for the Gx interface on the broadband gateway.

```

Action user@host> show unified-edge ggsn-pgw statistics gateway PGW apn apn-dynamic
Gateway: PGW
Control plane GTP statistics:
  Session establishment attempts:                21
  Successful session establishments:              20
  MS/peer initiated session deactivations:       12
  Successful MS/peer initiated deactivations:    12
  Gateway initiated session deactivations:       2
  Successful gateway initiated deactivations:    2
  MS initiated modification attempts:            0
  Successful MS initiated modifications:         0
  PGW/GGSN initiated modification attempts:      1
  Successful PGW/GGSN initiated modifications:   1
Redirect statistics:
  Successful apn redirects:                      0
  Attempted gateway redirects:                  0
  Successful gateway redirects:                 0
User authentication statistics:
  Authentication failures:                      0
  Attempted authentications:                   0
  Successful authentications:                  0
Address allocation statistics:
  Dynamic IP allocation attempts:               21
  Dynamic IP allocation success:                21
Charging statistics:
  Number of CDRs allocated:                    25
  Number of partial CDRs allocated:             0
  Number of CDRs closed:                      17
  Number of containers closed                  17
Static policy statistics:
  Session establishment attempts using static policy: 0
  Session establishment success using static policy: 0
DCCA-Gy Statistics:
  Online authorizations attempted:              0 Success : 0
  Online authorization timeouts:                0
  Quota threshold reauthorization requests sent: 0
Gy Diameter msg statistics:
  CCR-Initial Sent : 0 Success : 0 Fail : 0
  CCR-Update Sent : 0 Success : 0 Fail : 0
  CCR-Terminate Sent : 0 Success : 0 Fail : 0
  RAR Received : 0 Answer : 0 Fail : 0
  ASR Received : 0 Answer : 0
  CCR Failure :
    Transient : 0
    Parameter : 0
    Permanent : 0
    Unknown code : 0
    Unknown session : 0
Session Establishments Failed (by GTP cause):
  Others 0
  Service unavailable: 0
  System failure: 0
  No resources: 0
  No address: 0
  Service denied: 0
  Authentication Fail: 0
  APN access denied: 0
PCC Gx statistics:
  Session attempts:                21 Success: 20
  MS-peer initiated APN-AMBR modification attempts: 0 Success: 0
  MS-peer initiated QoS modification attempts: 0 Success: 0

```

```

        PCRF initiated session deactivations:          0
        Gateway initiated session deactivations:       2
        MS-peer initiated session deactivations:      12
Gx modification statistics:
    Initiated by MS-peer: 0          Success: 0
    Initiated by PCRF: 8           Success: 0
Modification event reason:
    QoS change: 0          RAT change: 0
    SGSN change: 0         SGW change: 0
    PLMN change: 0         RAI change: 0
    ULI change: 0          IP-CAN change: 0
    TFT change (MS): 0     TFT change (Network): 0
    Bearer loss: 0         Bearer recovery: 0
    Resource allocation: 0  Revalidation Timeout: 0
    QoS exceeding auth: 0  Time-of-Day procedure: 0
    Change of Subscription: 0 AMBR change: 0
    ECGI change: 0         TAI change: 0
    Timezone change: 0     Default-EPS-QoS change: 0
Dedicated bearer statistics:
    MS-peer initiated activation attempts: 0          Success: 0
    Network initiated activation attempts: 7          Success: 5
    MS-peer initiated modification attempts: 0         Success: 0
    Network initiated modification attempts: 0         Success: 0
    MS-peer initiated deactivations: 5
    Network initiated deactivations: 0
    Gateway initiated deactivations: 0
Gx Failure Statistics:
    GBR dedicated bearer create failure due to CAC: 0
    Non-GBR dedicated bearer create failure due to CAC: 0
    Session terminations due to unreachable PCRF: 0
    Session terminations due to PCRF restart: 0
Gx diameter message statistics:
    CCR-I sent: 21          CCA-I received: 20
    CCR-U sent: 20          CCA-U received: 20
    CCR-T sent: 15          CCA-T received: 0
    RAR received: 8         RAA sent: 6
    RAA sent resource failure: 0
CCR failure reason:
    Transient failure: 0          Initial params error: 0
    Permanent failure: 0         Unknown code: 0
    Unknown session: 0
Gx rule statistics:
    Dynamic rule activations: 0          Deactivations: 0
    Static rules activations: 10         Deactivations: 10
    Dynamic rule modifications: 20
Rule failure statistics:
    Rule validation failure: 14
    Rule enforcement failure no resource: 2
    Rule activation failure no resource: 0
    Rule update procedure fail: 0
Handover Statistics:
    Inter-RAT Handover attempts: 0          Success: 0
    Intra-RAT Handover attempts: 0          Success: 0
Data plane statistics:
    Total packets violating MIF ACL: 0
    Total accepted mobile-to-mobile packets: 0
    Total accepted mobile-to-mobile bytes: 0
Miscellaneous Packet statistics:
    IPv6 Router Solicitations received: 0
    IPv6 Router Advertisement transmitted: 0
    IPv6 Neighbor Solicitations received: 0

```



```

IPv6 Neighbor Advertisement transmitted:    0
Data plane GTP statistics (Gn/S5/S8):
  Input   packets:      0
  Input   bytes:        0
  Output  packets:      0
  Output  bytes:        0
  Discarded packets:    0
Data plane GTP statistics (Gi):
  Input   packets:      0
  Input   bytes:        0
  Output  packets:      0
  Output  bytes:        0
  Discarded packets:    0

```

**Meaning** The `show unified-edge ggsn-pgw statistics gateway PGW apn apn-dynamic` command displays the control plane Gx statistics for an APN. If the output shows that session attempts are successful, then the connection to the PCEF is functioning properly.

## Troubleshooting

To troubleshoot the policy and charging enforcement function (PCEF) configuration, perform these tasks:

- [Connection is Down Between the PCEF and PCRF on page 395](#)
- [PCEF and PCRF Application Messages Are Not Sent or Received on page 396](#)

### Connection is Down Between the PCEF and PCRF

**Problem** The connection between the PCEF and PCRF peers on the Gx interface appears to be down.

**Solution** To display Diameter peer status for the PCRF and PCEF:

1. From operational mode, enter the `show unified-edge ggsn-pgw diameter peer status` command.

```

user@host> show unified-edge ggsn-pgw diameter peer status
Gateway: PGW
Control plane GTP statistics:
  Session establishment attempts:      6
  Successful session establishments:    6
  MS/peer initiated session deactivations: 4
  Successful MS/peer initiated deactivations: 4
  Gateway initiated session deactivations: 0
  Successful gateway initiated deactivations: 0
PCC Gx statistics:
  Session attempts using dynamic policy: 6      Success: 6
  Dedicated bearer activation attempts:  5      Success: 3
  MS-Peer init dedicated bearer deactivations: 2
  Gateway init dedicated bearer deactivations: 0
  PCRF init dedicated bearer deactivations: 0
Data plane global statistics:
  Source address violation packets:      0
  Non-existent TEID/TID packets:        0
  GTP length error packets:              0
  Non-existent UE address packets:       0
  Mobile-to-mobile packets:              0

```

```

Data plane GTP statistics (Gn/S5/S8):
  Input   packets:      15
  Input   bytes:       1500
  Output  packets:      15
  Output  bytes:       1500
  Discarded packets:    0
Data plane GTP statistics (Gi):
  Input   packets:      15
  Input   bytes:       1500
  Output  packets:      15
  Output  bytes:       1500
  Discarded packets:    0

```

2. Check that status of the State field, which is displayed at the beginning of the output. When the connection between the Diameter peers (PCEF and PCRF) is up, the State status indicates **I-Open**.
3. Check that the status of the Watchdog State field, which is displayed near the beginning of the output. When Diameter peers are connected, the Watchdog State status indicates **okay**.

### PCEF and PCRF Application Messages Are Not Sent or Received

**Problem** The PCRF and PCEF application messages (Re-Authorization Request/Re-Authorization Answer or Credit Control Request/Credit Control Answer) are not being sent or received.

**Solution** To display status of application messages for the PCRF and PCEF:

1. From operational mode, enter the **show unified-edge ggsn-pgw diameter peer statistics** command.

```

user@host> show unified-edge ggsn-pgw diameter peer statistics
Peer: p1
Request Timeouts:                0
Request Retransmissions:         0
Messages                         Transmitted      Received
-----
Total Messages                   22              22
Credit Control Requests         14              0
Credit Control Answers          0              14
Re-Auth Requests                 0              2
Re-Auth Answers                  2              0
Abort Session Requests           0              0
Abort Session Answers            0              0
Capability Exchange Requests     2              0
Capability Exchange Answers      0              2
Device Watchdog Requests         4              0
Device Watchdog Answers          0              4
Disconnect Peer Requests         0              0
Disconnect Peer Answers          0              0

```

2. Check that for each message type, there are an equal number of messages for requests and answers.

**Related Documentation** • [Application-Aware Policy and Charging Control Rules Overview on page 353](#)

- [Example: Configuring Policy and Charging Enforcement Function with Application-Aware Policy and Charging Control Rules on page 397](#)
- [Policy and Charging Control Rules Overview on page 349](#)
- [Policy and Charging Enforcement Function Overview on page 347](#)
- [Understanding Event Triggers on page 363](#)
- [Understanding How Dynamic and Static Policy and Charging Control Rules Are Provisioned on page 359](#)

## Example: Configuring Policy and Charging Enforcement Function with Application-Aware Policy and Charging Control Rules

---

This example shows how to configure the policy and charging enforcement function (PCEF) with application-aware policy and charging control (PCC) rules on the MobileNext Broadband Gateway. To enforce application-aware PCC rules, PCEF is applied as a service on the APN (the MIF interface) to indicate to the Packet Forwarding Engine that traffic should be directed to the Junos OS services PIC that hosts the PCEF service. When subscriber traffic is redirected to the services PIC, processing is completed and the appropriate policies are applied as a service on the MIF interface associated with an APN.

- [Requirements on page 397](#)
- [Overview on page 398](#)
- [Configuration on page 398](#)
- [Verification on page 418](#)
- [Troubleshooting on page 424](#)

### Requirements

This example uses the following hardware and software components:

- A supported MX Series chassis configured with supported line cards and a services PIC
- A supported and properly installed version of 64-bit Junos OS and the **jmobile** software package
- Correct configuration as a P-GW with corresponding interfaces

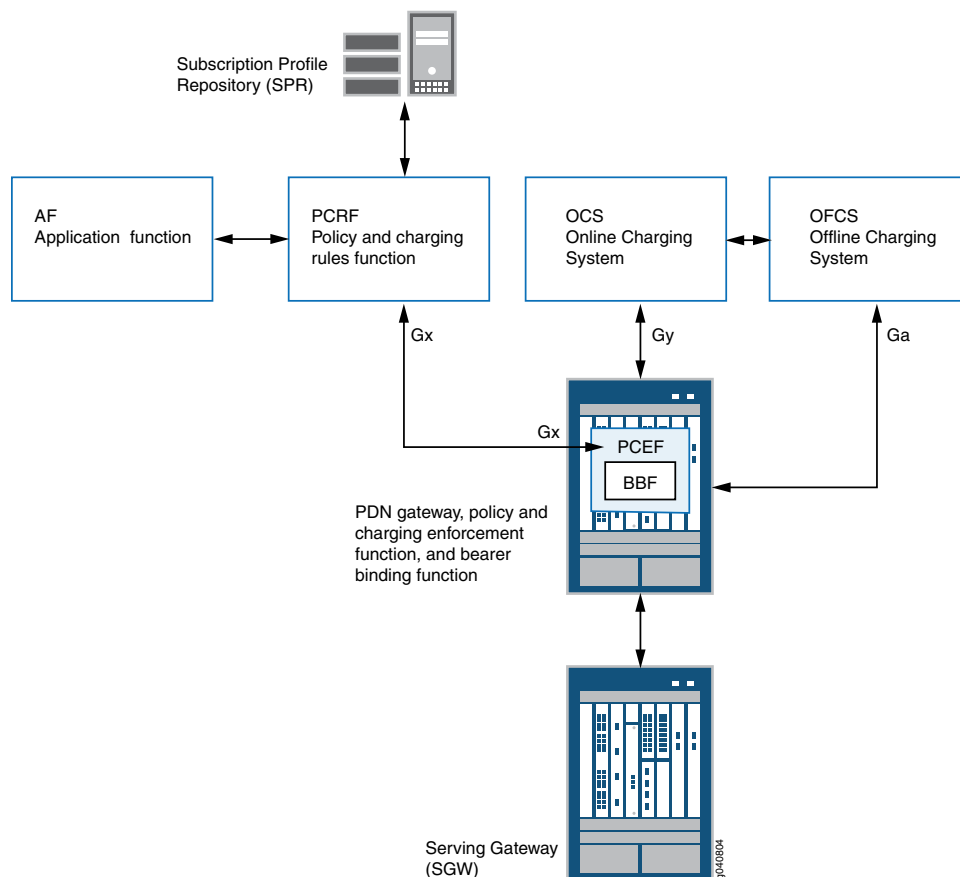
Before you begin:

- Configure GTP and Diameter.
- Configure mobile interfaces for access point names (APNs).
- Configure APNs.
- Configure the policy and charging rule function (PCRF).

## Overview

The PCEF is part of a complete broadband gateway configuration, including online and offline charging, and quality-of-service (QoS) determination. The Gx interface connects the PCEF and the PCRF.

**Figure 52: Architecture for Policy and Charging Enforcement Function**



## Topology

The topology for this PCEF example consists of mobile network nodes and the interfaces connecting them. The key component is the PCEF, which enforces policy decisions that are received from the PCRF and provides the PCRF with user and access information over the Gx reference point. The PCEF also interacts with the Online Charging System (OCS), which provides credit management for prepaid charging, and reports resource usage to the Offline Charging System (OFCS).

## Configuration

To configure the PCEF on the P-GW, perform these tasks:

- [Configuring Application Signatures on page 399](#)
- [Configuring an Application Identification Profile on page 400](#)

- [Configuring PCEF Services for Application-Aware Traffic on page 400](#)
- [Configuring Service Data Flow Filters on page 402](#)
- [Configuring PCC Action Profiles on page 403](#)
- [Configuring Application-Aware PCC Rules on page 409](#)
- [Configuring PCC Rulebases on page 412](#)
- [Configuring a Diameter Gx Profile for Dynamic Services on page 413](#)
- [Configuring PCEF Profiles for Dynamic Policies on page 413](#)
- [Configuring PCEF Profiles for Static \(Local\) Services on page 415](#)
- [Applying PCEF Policies for Dynamic Services to APNs on page 417](#)
- [Applying a PCEF Profile for Static Services to an APN on page 417](#)
- [Results on page 418](#)

### Configuring Application Signatures

#### CLI Quick Configuration

To quickly configure application signatures to detect Layer 7 nested applications, copy the following commands and paste them into the router terminal window:

```
[edit services application-identification]
set download url https://devdb.secteam.juniper.net/xmlexport.cgi
set nested-application reddy protocol HTTP
set nested-application reddy signature reddy member m01 context http-url-parsed
set nested-application reddy signature reddy member m01 pattern ".*\[reddy\].*"
set nested-application reddy signature reddy member m01 direction client-to-server
set nested-application reddy signature reddy maximum-transactions 1
```

#### Step-by-Step Procedure

The application identification (APPID) feature (supported on MX Series routers equipped with Multiservices DPCs) identifies applications as constituents of application groups in TCP, UDP, or ICMP traffic. For more information about defining the application signatures in the application identification engine, see “Configuring Application Identification for Nested Applications” in the Junos OS *Services Interfaces* guide.

1. Specify the URL to download the Junos OS application package:

```
[edit services application-identification]
user@host# set download url https://devdb.secteam.juniper.net/xmlexport.cgi
```

2. Configure a custom nested application definition for the desired application name that will be used by the system to identify the nested application as it passes through the device.

```
[edit services application-identification nested-application]
user@host# set reddy protocol HTTP
user@host# set reddy signature reddy member m01 context http-url-parsed
user@host# set reddy signature reddy member m01 pattern ".*\[reddy\].*"
user@host# set reddy signature reddy member m01 direction client-to-server
user@host# set reddy signature reddy maximum-transactions 1
```

### Configuring an Application Identification Profile

---

**CLI Quick Configuration** To quickly configure an application identification profile, copy the following commands and paste them into the router terminal window:

```
[edit services application-identification]
edit profile app-id-profile1
```

**Step-by-Step Procedure** You configure an application profile for use in a service set. The profile consists of one or more rule sets, but only one profile can be included per service set. For more information, see “Configuring Application Profiles” in the Junos OS *Services Interfaces* documentation.

1. Define an application profile for use in the *dpi-service-set-1* service set.

```
[edit services application-identification]
user@host# edit profile app-id-profile1
```

### Configuring PCEF Services for Application-Aware Traffic

---

**CLI Quick Configuration**

```
[edit unified-edge gateways ggsn-pgw PGW1 system]
set service-pics interface ams0
[edit services pcef profile pcef-service-profile1]
[edit services service-set dpi-service-set-1]
set tcp-mss 1300
set service-set-options subscriber-awareness
set pcef-profile pcef-service-profile-1
set application-identification app-id-profile1
set interface-service service-interface ams0
[edit interfaces mif unit 0 family inet service]
set input service-set dpi-service-set-1
set output service-set dpi-service-set-1
[edit interfaces mif unit 1 family inet service]
set input service-set dpi-service-set-1
set output service-set dpi-service-set-1
[edit interfaces mif unit 2 family inet service]
set input service-set dpi-service-set-1
set output service-set dpi-service-set-1
[edit interfaces mif unit 3 family inet service]
set input service-set dpi-service-set-1
set output service-set dpi-service-set-1
[edit firewall family inet service-filter dpi-filter-1]
set term dpi-flow-1 from redirect-reason dpi
set term dpi-flow-1 then service
[edit interfaces mif unit 0]
set clear-dont-fragment-bit
set family inet service input service-set dpi-service-set-1 service-filter dpi-filter-1
set family inet service output service-set dpi-service-set-1 service-filter dpi-filter-1
[edit interfaces mif unit 1]
set clear-dont-fragment-bit
set family inet service input service-set dpi-service-set-1 service-filter dpi-filter-1
set family inet service output service-set dpi-service-set-1 service-filter dpi-filter-1
[edit interfaces mif unit 2]
set clear-dont-fragment-bit
set family inet service input service-set dpi-service-set-1 service-filter dpi-filter-1
```

```

set family inet service output service-set dpi-service-set-1 service-filter dpi-filter-1
[edit interfaces mif unit 3]
set clear-dont-fragment-bit
set family inet service input service-set dpi-service-set-1 service-filter dpi-filter-1
set family inet service output service-set dpi-service-set-1 service-filter dpi-filter-1

```

### Step-by-Step Procedure

To configure an application-aware PCEF service for an APN:

1. Configure a service PIC for the PCEF service.  

```

[edit unified-edge gateways ggsn-pgw PGW1 system]
user@host# set service-pics interface ams0

```
2. Configure the PCEF services profile by specifying a name for the PCEF profile.  

```

[edit ]
user@host# edit services pcef profile pcef-service-profile1

```



**NOTE:** In this release, the PCEF profile is a placeholder profile with no configuration options; however, you must create a PCEF profile to provide future compatibility for PCEF services.

3. Define a service to use as an application-aware PCEF service.  

```

[edit services service-set dpi-service-set-1]
user@host# set tcp-mss 1300
user@host# set service-set-options subscriber-awareness
user@host# set pcef-profile pcef-service-profile1
user@host# set application-identification app-id-profile1
user@host# set interface-service service-interface ams1.1

```
4. Apply the PCEF application-aware service to the mobile interfaces for the APNs for both ingress and egress traffic so that all traffic arriving on the APN is inspected for application-based charging and policy.  

```

[edit interfaces mif unit 0 family inet service]
user@host# set input service-set dpi-service-set-1
user@host# set output service-set dpi-service-set-1
[edit interfaces mif unit 1 family inet service]
user@host# set input service-set dpi-service-set-1
user@host# set output service-set dpi-service-set-1
[edit interfaces mif unit 2 family inet service]
user@host# set input service-set dpi-service-set-1
user@host# set output service-set dpi-service-set-1
[edit interfaces mif unit 3 family inet service]
user@host# set input service-set dpi-service-set-1
user@host# set output service-set dpi-service-set-1

```
5. Configure a Deep Packet Inspection (DPI) filter for application-aware traffic.  

```

[edit ]
user@host# edit firewall family inet service-filter dpi-filter-1
[edit firewall family inet service-filter dpi-filter-1]
user@host# set term dpi-flow-1 from redirect-reason dpi
user@host# set term dpi-flow-1 then service

```

6. Apply the DPI filter to the MIF interfaces so that only application-aware traffic is forwarded to the services PICs.

```
[edit interfaces mif unit 0]
user@host# set clear-dont-fragment-bit
user@host# set family inet service input service-set dpi-service-set-1 service-filter
dpi-filter-1
user@host# set family inet service output service-set dpi-service-set-1 service-filter
dpi-filter-1
[edit interfaces mif unit 1]
user@host# set clear-dont-fragment-bit
user@host# set family inet service input service-set dpi-service-set-1 service-filter
dpi-filter-1
user@host# set family inet service output service-set dpi-service-set-1 service-filter
dpi-filter-1
[edit interfaces mif unit 2]
user@host# set clear-dont-fragment-bit
user@host# set family inet service input service-set dpi-service-set-1 service-filter
dpi-filter-1
user@host# set family inet service output service-set dpi-service-set-1 service-filter
dpi-filter-1
[edit interfaces mif unit 3]
user@host# set clear-dont-fragment-bit
user@host# set family inet service input service-set dpi-service-set-1 service-filter
dpi-filter-1
user@host# set family inet service output service-set dpi-service-set-1 service-filter
dpi-filter-1
```

7. Include the `jservice-appid`, `jservice-pcef`, and `jservice-mss` packages with the services PIC configuration.

```
[edit chassis fpc 1 pic 0 adaptive-services service-package extension-provider]
user@host# set package jservices-appid
user@host# set package jservices-mss
user@host# set package jservices-pcef
[edit chassis fpc 1 pic 1 adaptive-services service-package extension-provider]
user@host# set package jservices-appid
user@host# set package jservices-mss
user@host# set package jservices-pcef
```

---

### Configuring Service Data Flow Filters

---

**CLI Quick Configuration** To quickly configure the service data flow filters, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge pcef flow-descriptions allow_all]
set direction both
[edit unified-edge pcef flow-descriptions flow-tcp-1]
set direction both
set protocol 6
```

**Step-by-Step Procedure** To configure the service data flow filters:

1. Configure a service data flow filter to provide a wildcard PCC rule that permits all traffic.



```
[edit]
user@host# set unified-edge pcef flow-descriptions allow_all direction both
```



**NOTE:** You can configure a wild-card service data flow filter in an application-aware PCC rule, so that any flows redirected to the PCEF service that do not match any of the configured application-aware PCC rules are appropriately handled and assigned a rating group.

2. Configure a service data flow filter to specify a protocol in an application-aware PCC rule.

```
[edit]
user@host# set unified-edge pcef flow-descriptions flow-tcp-1 direction both
user@host# set unified-edge pcef flow-descriptions flow-tcp-1 protocol 6
```

### Configuring PCC Action Profiles

#### CLI Quick Configuration

To quickly configure the Policy and Charging Control (PCC) action profiles, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge pcef pcc-action-profiles pap-1]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 10
set charging charging-method offline
[edit unified-edge pcef pcc-action-profiles pap-2]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 11
set charging charging-method offline
[edit unified-edge pcef pcc-action-profiles pap-11]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 20
set charging charging-method online
[edit unified-edge pcef pcc-action-profiles pap-12]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 21
set charging charging-method online
```

```
[edit unified-edge pcef pcc-action-profiles pap-6]
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status disable-both
set charging rating-group 15
set charging charging-method offline
[edit unified-edge pcef pcc-action-profiles pap-7]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 16
set charging charging-method offline
[edit unified-edge pcef pcc-action-profiles pap-16]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 25
set charging service-identifier 25
set charging charging-method online
[edit unified-edge pcef pcc-action-profiles pap-17]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 26
set charging service-identifier 26
set charging charging-method online
[edit unified-edge pcef pcc-action-profiles pap-3]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 12
set charging charging-method offline
[edit unified-edge pcef pcc-action-profiles pap-13]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 22
set charging charging-method online
[edit unified-edge pcef pcc-action-profiles pap-4]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 13
```

```

set charging charging-method offline
[edit unified-edge pcef pcc-action-profiles pap-5]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 14
set charging charging-method offline
[edit unified-edge pcef pcc-action-profiles pap-14]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 23
set charging charging-method online
[edit unified-edge pcef pcc-action-profiles pap-15]
set qci 5
set allocation-retention-priority priority-level 1
set allocation-retention-priority preemption-capability 0
set allocation-retention-priority preemption-vulnerability 0
set gate-status uplink-downlink
set charging rating-group 24
set charging charging-method online

```

#### Step-by-Step Procedure

To configure the PCC action profiles:

1. Configure the PCC action profiles for static (local) PCC rules for offline-charging traffic.

```

[edit]
user@host# set unified-edge pcef pcc-action-profiles pap-1 qci 5
user@host# set unified-edge pcef pcc-action-profiles pap-1
allocation-retention-priority priority-level 1
user@host# set unified-edge pcef pcc-action-profiles pap-1
allocation-retention-priority preemption-capability 0
user@host# set unified-edge pcef pcc-action-profiles pap-1
allocation-retention-priority preemption-vulnerability 0
user@host# set unified-edge pcef pcc-action-profiles pap-1 gate-status
uplink-downlink
user@host# set unified-edge pcef pcc-action-profiles pap-1 set charging rating-group
10
user@host# set unified-edge pcef pcc-action-profiles pap-1 set charging
charging-method offline
user@host# set unified-edge pcef pcc-action-profiles pap-2 qci 5
user@host# set unified-edge pcef pcc-action-profiles pap-2
allocation-retention-priority priority-level 1
user@host# set unified-edge pcef pcc-action-profiles pap-2
allocation-retention-priority preemption-capability 0
user@host# set unified-edge pcef pcc-action-profiles pap-2
allocation-retention-priority preemption-vulnerability 0
user@host# set unified-edge pcef pcc-action-profiles pap-2 gate-status
uplink-downlink
user@host# set unified-edge pcef pcc-action-profiles pap-2 set charging rating-group
11

```

```
user@host# set unified-edge pcef pcc-action-profiles pap-2 set charging
charging-method offline
```

2. Configure the PCC action profiles for static PCC rules for online-charging traffic.

```
[edit]
user@host# set unified-edge pcef pcc-action-profiles pap-11 qci 5
user@host# set unified-edge pcef pcc-action-profiles pap-11
allocation-retention-priority priority-level 1
user@host# set unified-edge pcef pcc-action-profiles pap-11
allocation-retention-priority preemption-capability 0
user@host# set unified-edge pcef pcc-action-profiles pap-11
allocation-retention-priority preemption-vulnerability 0
user@host# set unified-edge pcef pcc-action-profiles pap-11 gate-status
uplink-downlink
user@host# set unified-edge pcef pcc-action-profiles pap-11 charging rating-group
20
user@host# set unified-edge pcef pcc-action-profiles pap-11 charging
charging-method online
user@host# set unified-edge pcef pcc-action-profiles pap-12 qci 5
user@host# set unified-edge pcef pcc-action-profiles pap-12
allocation-retention-priority priority-level 1
user@host# set unified-edge pcef pcc-action-profiles pap-12
allocation-retention-priority preemption-capability 0
user@host# set unified-edge pcef pcc-action-profiles pap-12
allocation-retention-priority preemption-vulnerability 0
user@host# set unified-edge pcef pcc-action-profiles pap-12 gate-status
uplink-downlink
user@host# set unified-edge pcef pcc-action-profiles pap-12 charging rating-group
21
user@host# set unified-edge pcef pcc-action-profiles pap-12 charging
charging-method online
```

3. Configure the PCC action profiles for static-Gx PCC rules for offline-charging traffic.

```
[edit]
user@host# set unified-edge pcef pcc-action-profiles pap-6 qci 5
user@host# set unified-edge pcef pcc-action-profiles pap-6
allocation-retention-priority priority-level 1
user@host# set unified-edge pcef pcc-action-profiles pap-6
allocation-retention-priority preemption-capability 0
user@host# set unified-edge pcef pcc-action-profiles pap-6
allocation-retention-priority preemption-vulnerability 0
user@host# set unified-edge pcef pcc-action-profiles pap-6 gate-status disable-both
user@host# set unified-edge pcef pcc-action-profiles pap-6 charging rating-group
15
user@host# set unified-edge pcef pcc-action-profiles pap-6 charging
charging-method offline
user@host# set unified-edge pcef pcc-action-profiles pap-6
user@host# set unified-edge pcef pcc-action-profiles pap-7 qci 5
user@host# set unified-edge pcef pcc-action-profiles pap-7
allocation-retention-priority priority-level 1
user@host# set unified-edge pcef pcc-action-profiles pap-7
allocation-retention-priority preemption-capability 0
user@host# set unified-edge pcef pcc-action-profiles pap-7
allocation-retention-priority preemption-vulnerability 0
```

```

user@host# set unified-edge pcef pcc-action-profiles pap-7 gate-status
uplink-downlink
user@host# set unified-edge pcef pcc-action-profiles pap-7 charging rating-group
16
user@host# set unified-edge pcef pcc-action-profiles pap-7 charging
charging-method offline

```

4. Configure the PCC action profiles for static-Gx PCC rules for online-charging traffic.

```

[edit]
user@host# set unified-edge pcef pcc-action-profiles pap-16 qci 5
user@host# set unified-edge pcef pcc-action-profiles pap-16
allocation-retention-priority priority-level 1
user@host# set unified-edge pcef pcc-action-profiles pap-16
allocation-retention-priority preemption-capability 0
user@host# set unified-edge pcef pcc-action-profiles pap-16
allocation-retention-priority preemption-vulnerability 0
user@host# set unified-edge pcef pcc-action-profiles pap-16 gate-status
uplink-downlink
user@host# set unified-edge pcef pcc-action-profiles pap-16 charging rating-group
25
user@host# set unified-edge pcef pcc-action-profiles pap-16 charging
service-identifier 25
user@host# set unified-edge pcef pcc-action-profiles pap-16 charging
charging-method online
user@host# set unified-edge pcef pcc-action-profiles pap-17 qci 5
user@host# set unified-edge pcef pcc-action-profiles pap-17
allocation-retention-priority priority-level 1
user@host# set unified-edge pcef pcc-action-profiles pap-17
allocation-retention-priority preemption-capability 0
user@host# set unified-edge pcef pcc-action-profiles pap-17
allocation-retention-priority preemption-vulnerability 0
user@host# set unified-edge pcef pcc-action-profiles pap-17 gate-status
uplink-downlink
user@host# set unified-edge pcef pcc-action-profiles pap-17 charging rating-group
26
user@host# set unified-edge pcef pcc-action-profiles pap-17 charging
service-identifier 26
user@host# set unified-edge pcef pcc-action-profiles pap-17 charging
charging-method online

```

5. Configure the PCC action profiles for wildcard rules for offline-charging traffic.

```

[edit]
user@host# set unified-edge pcef pcc-action-profiles pap-3 qci 5
user@host# set unified-edge pcef pcc-action-profiles pap-3
allocation-retention-priority priority-level 1
user@host# set unified-edge pcef pcc-action-profiles pap-3
allocation-retention-priority preemption-capability 0
user@host# set unified-edge pcef pcc-action-profiles pap-3
allocation-retention-priority preemption-vulnerability 0
user@host# set unified-edge pcef pcc-action-profiles pap-3 gate-status
uplink-downlink
user@host# set unified-edge pcef pcc-action-profiles pap-3 charging rating-group
12
user@host# set unified-edge pcef pcc-action-profiles pap-3 charging
charging-method offline

```

6. Configure the PCC action profiles for wildcard rules for online-charging traffic.

```
[edit]
user@host# set unified-edge pcef pcc-action-profiles pap-13 qci 5
user@host# set unified-edge pcef pcc-action-profiles pap-13
  allocation-retention-priority priority-level 1
user@host# set unified-edge pcef pcc-action-profiles pap-13
  allocation-retention-priority preemption-capability 0
user@host# set unified-edge pcef pcc-action-profiles pap-13
  allocation-retention-priority preemption-vulnerability 0
user@host# set unified-edge pcef pcc-action-profiles pap-13 gate-status
  uplink-downlink
user@host# set unified-edge pcef pcc-action-profiles pap-13 charging rating-group
  22
user@host# set unified-edge pcef pcc-action-profiles pap-13 charging
  charging-method online
```

7. Configure the PCC action profiles for static rules for a rulebase for offline-charging traffic.

```
[edit]
user@host# set unified-edge pcef pcc-action-profiles pap-4 qci 5
user@host# set unified-edge pcef pcc-action-profiles pap-4
  allocation-retention-priority priority-level 1
user@host# set unified-edge pcef pcc-action-profiles pap-4
  allocation-retention-priority preemption-capability 0
user@host# set unified-edge pcef pcc-action-profiles pap-4
  allocation-retention-priority preemption-vulnerability 0
user@host# set unified-edge pcef pcc-action-profiles pap-4 gate-status
  uplink-downlink
user@host# set unified-edge pcef pcc-action-profiles pap-4 charging rating-group
  13
user@host# set unified-edge pcef pcc-action-profiles pap-4 charging
  charging-method offline
user@host# set unified-edge pcef pcc-action-profiles pap-5 qci 5
user@host# set unified-edge pcef pcc-action-profiles pap-5
  allocation-retention-priority priority-level 1
user@host# set unified-edge pcef pcc-action-profiles pap-5
  allocation-retention-priority preemption-capability 0
user@host# set unified-edge pcef pcc-action-profiles pap-5
  allocation-retention-priority preemption-vulnerability 0
user@host# set unified-edge pcef pcc-action-profiles pap-5 gate-status
  uplink-downlink
user@host# set unified-edge pcef pcc-action-profiles pap-5 charging rating-group
  14
user@host# set unified-edge pcef pcc-action-profiles pap-5 charging
  charging-method offline
```

8. Configure the PCC action profiles for static rules for a rulebase for online-charging traffic.

```
[edit]
user@host# set unified-edge pcef pcc-action-profiles pap-14 qci 5
user@host# set unified-edge pcef pcc-action-profiles pap-14
  allocation-retention-priority priority-level 1
user@host# set unified-edge pcef pcc-action-profiles pap-14
  allocation-retention-priority preemption-capability 0
```

```

user@host# set unified-edge pcef pcc-action-profiles pap-14
allocation-retention-priority preemption-vulnerability 0
user@host# set unified-edge pcef pcc-action-profiles pap-14 gate-status
uplink-downlink
user@host# set unified-edge pcef pcc-action-profiles pap-14 charging-rating-group
23
user@host# set unified-edge pcef pcc-action-profiles pap-14 charging
charging-method online
user@host# set unified-edge pcef pcc-action-profiles pap-15 qci 5
user@host# set unified-edge pcef pcc-action-profiles pap-15
allocation-retention-priority priority-level 1
user@host# set unified-edge pcef pcc-action-profiles pap-15
allocation-retention-priority preemption-capability 0
user@host# set unified-edge pcef pcc-action-profiles pap-15
allocation-retention-priority preemption-vulnerability 0
user@host# set unified-edge pcef pcc-action-profiles pap-15 gate-status
uplink-downlink
user@host# set unified-edge pcef pcc-action-profiles pap-15 charging-rating-group
24
user@host# set unified-edge pcef pcc-action-profiles pap-15 charging
charging-method online

```

### Configuring Application-Aware PCC Rules

**CLI Quick Configuration** To quickly configure PCC rules, copy the following commands and paste them into the router terminal window:

```

[edit unified-edge pcef pcc-rules local-offline-rule-1]
set from flows allow_all
set from applications junos:http
set from nested-applications reddy
set then pcc-action-profile pap-1
[edit unified-edge pcef pcc-rules local-offline-rule-2]
set from flows allow_all
set from applications junos:http
set from nested-applications junos:FACEBOOK-ACCESS
set then pcc-action-profile pap-2
[edit unified-edge pcef pcc-rules local-offline-wildcard-rule]
set from flows allow_all
set then pcc-action-profile pap-3
[edit unified-edge pcef pcc-rules local-online-rule-1]
set from flows flow-tcp-1
set from applications junos:http
set from nested-applications reddy
set then pcc-action-profile pap-11
[edit unified-edge pcef pcc-rules local-online-rule-2]
set from flows flow-tcp-1
set from applications junos:http
set from nested-applications junos:FACEBOOK-ACCESS
set then pcc-action-profile pap-12
[edit unified-edge pcef pcc-rules local-online-wildcard-rule]
set from flows allow_all
set then pcc-action-profile pap-13
[edit unified-edge pcef pcc-rules local-offline-rb-rule-1]
set from flows allow_all

```

```
set from applications junos:http
set from nested-applications junos:LINKEDIN
set then pcc-action-profile pap-4
[edit unified-edge pcef pcc-rules local-offline-rb-rule-2]
set from flows allow_all
set from applications junos:http
set from nested-applications junos:YAHOO-MAIL
set then pcc-action-profile pap-5
[edit unified-edge pcef pcc-rules local-online-rb-rule-1]
set from flows flow-tcp-1
set from applications junos:http
set from nested-applications junos:LINKEDIN
set then pcc-action-profile pap-14
[edit unified-edge pcef pcc-rules local-online-rb-rule-2]
set from flows flow-tcp-1
set from applications junos:http
set from nested-applications junos:YAHOO-MAIL
set then pcc-action-profile pap-15
[edit unified-edge pcef pcc-rulebases local-offline-rb-1]
set pcc-rule local-offline-rb-rule-1 precedence 3001
set local-offline-rb-1 pcc-rule local-offline-rb-rule-2 precedence 3010
[edit unified-edge pcef pcc-rulebases local-online-rb-1]
set pcc-rule local-online-rb-rule-1 precedence 3501
set pcc-rule local-online-rb-rule-2 precedence 3510
[edit unified-edge pcef pcc-rules static-gx-offline-rule-1]
set from flows flow-tcp-1
set from applications junos:http
set from nested-applications reddy
set then pcc-action-profile pap-6
[edit unified-edge pcef pcc-rules static-gx-offline-rule-2]
set from flows flow-tcp-1
set from applications junos:http
set from nested-applications junos:FACEBOOK-ACCESS
set then pcc-action-profile pap-7
[edit unified-edge pcef pcc-rules static-gx-offline-wildcard-rule]
set from flows allow_all
set then pcc-action-profile pap-8
[edit unified-edge pcef pcc-rules static-gx-online-rule-1]
set from flows allow_all
set from applications junos:http
set from nested-applications reddy
set then pcc-action-profile pap-16
[edit unified-edge pcef pcc-rules static-gx-online-rule-2]
set from flows allow_all
set from applications junos:http
set from nested-applications junos:FACEBOOK-ACCESS
set then pcc-action-profile pap-17
[edit set unified-edge pcef pcc-rules static-gx-online-wildcard-rule]
set from flows allow_all
set then pcc-action-profile pap-18
```

**Step-by-Step  
Procedure**

To configure application-aware PCC rules for the MobileNext Broadband Gateway:

1. Configure static PCC rules for offline-charging traffic.

```
[edit unified-edge pcef pcc-rules local-offline-rule-1]
```



```

user@host# set from flows allow_all
user@host# set from applications junos:http
user@host# set from nested-applications reddy
user@host# set then pcc-action-profile pap-1
[edit unified-edge pcef pcc-rules local-offline-rule-2]
user@host# set from flows allow_all
user@host# set from applications junos:http
user@host# set from nested-applications junos:FACEBOOK-ACCESS
user@host# set then pcc-action-profile pap-2

```

2. Configure static PCC rules to include in a rulebase for offline-charging traffic.

```

[edit unified-edge pcef pcc-rules local-offline-rb-rule-1]
user@host# set from flows allow_all
user@host# set from applications junos:http
user@host# set from nested-applications junos:LINKEDIN
user@host# set then pcc-action-profile pap-4
[edit unified-edge pcef pcc-rules local-offline-rb-rule-2]
user@host# set from flows allow_all
user@host# set from applications junos:http
user@host# set from nested-applications junos:YAHOO-MAIL
user@host# set then pcc-action-profile pap-5
[edit unified-edge pcef pcc-rules local-offline-rule-1]
user@host# set from flows allow_all
user@host# set from applications junos:http
user@host# set from nested-applications reddy
user@host# set then pcc-action-profile pap-1
[edit unified-edge pcef pcc-rules local-offline-rule-2]
user@host# set from flows allow_all
user@host# set from applications junos:http
user@host# set from nested-applications junos:FACEBOOK-ACCESS
user@host# set then pcc-action-profile pap-2

```

3. Configure a default Layer 3 or Layer 4 wildcard PCC rule for offline-charging traffic to ensure that the default charging characteristics are applied to unmatched subscriber traffic without dropping that traffic.

```

[edit unified-edge pcef pcc-rules local-offline-wildcard-rule]
user@host# set from flows allow_all
user@host# set then pcc-action-profile pap-3

```



**NOTE:** The PCEF profile that includes application-aware PCC rules must also include a wildcard Layer 3 or Layer 4 PCC rule at a lower precedence.

4. Configure the static PCC rules for online traffic.

```

[edit unified-edge pcef pcc-rules local-online-rule-1]
user@host# set from flows flow-tcp-1
user@host# set from applications junos:http
user@host# set from nested-applications reddy
user@host# set then pcc-action-profile pap-11
[edit unified-edge pcef pcc-rules local-online-rule-2]
user@host# set from flows flow-tcp-1

```

```
user@host# set from applications junos:http
user@host# set from nested-applications junos:FACEBOOK-ACCESS
user@host# set then pcc-action-profile pap-12
```

5. Configure static PCC rules to include in a rulebase for online traffic.

```
[edit unified-edge pcef pcc-rules local-online-rb-rule-1]
user@host# set from flows flow-tcp-1
user@host# set from applications junos:http
user@host# set from nested-applications junos:LINKEDIN
user@host# set then pcc-action-profile pap-14
[edit unified-edge pcef pcc-rules local-online-rb-rule-2]
user@host# set from flows flow-tcp-1
user@host# set from applications junos:http
user@host# set from nested-applications junos:YAHOO-MAIL
user@host# set then pcc-action-profile pap-15
```

6. Configure a default Layer 3 or Layer 4 wildcard PCC rule for online traffic to ensure that the default charging characteristics are applied to unmatched subscriber traffic without dropping that traffic.

```
[edit unified-edge pcef pcc-rules local-online-wildcard-rule]
user@host# set from flows allow_all
user@host# set then pcc-action-profile pap-13
```

### Configuring PCC Rulebases

---

#### CLI Quick Configuration

To quickly configure a PCC rulebase, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge pcef pcc-rulebases local-offline-rb-1]
set pcc-rule local-offline-rb-rule-1 precedence 3001
set pcc-rule local-offline-rb-rule-2 precedence 3010
[edit unified-edge pcef pcc-rulebases local-online-rb-1]
set pcc-rule local-online-rb-rule-1 precedence 3501
set pcc-rule local-online-rb-rule-2 precedence 3510
```

#### Step-by-Step Procedure

To configure PCC rulebases:

1. Specify a name for the local rulebases you want to configure to manage online-charging traffic and offline-charging traffic.

```
[edit]
user@host# edit unified-edge pcef pcc-rulebases local-offline-rb-1
user@host# edit unified-edge pcef pcc-rulebases local-online-rb-1
```

2. Specify the PCC rules that each rulebase references and assign a precedence for each PCC rule.

```
[edit unified-edge pcef pcc-rulebases local-offline-rb-1]
user@host# set pcc-rule local-offline-rb-rule-1 precedence 3001
user@host# set pcc-rule local-offline-rb-rule-2 precedence 3010
[edit unified-edge pcef pcc-rulebases local-online-rb-1]
user@host# set pcc-rule local-online-rb-rule-1 precedence 3501
user@host# set pcc-rule local-online-rb-rule-2 precedence 3510
```



**NOTE:** The higher the precedence value the lower the precedence and vice-versa. In this example, the PCC rule with precedence 3001 is evaluated first and then the PCC rule with precedence 3010 is evaluated, and so on.

### Configuring a Diameter Gx Profile for Dynamic Services

**CLI Quick Configuration** To quickly configure a Gx profile, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge diameter-profiles gx-profile gx1]
set targets pcef-dne1 destination-realm juniper.net
set targets pcef-dne1 priority 1
set targets pcef-dne1 network-element pcrf-dne1
set targets pcef-dne2 destination-realm juniper.net
set targets pcef-dne2 priority 1
set targets pcef-dne2 network-element pcrf-dne2
```

**Step-by-Step Procedure** To configure the Diameter Gx profile named *gx1* for the Gx application:

1. Specify a name for the Gx profile.  

```
[edit unified-edge diameter-profiles]
user@host# edit gx-profile gx1
```
2. Configure the target named *pcef-dne1* for the profile and specify its destination realm, priority, and network element.  

```
[edit unified-edge diameter-profiles gx-profile gx1]
user@host# set targets pcef-dne1 destination-realm juniper.net
user@host# set targets pcef-dne1 priority 1
user@host# set targets pcef-dne1 network-element pcrf-dne1
```
3. Configure the target named *pcef-dne2* for the profile and specify its destination realm, priority, and network element.  

```
[edit unified-edge diameter-profiles gx-profile gx1]
user@host# set targets pcef-dne2 destination-realm juniper.net
user@host# set targets pcef-dne2 priority 1
user@host# set targets pcef-dne2 network-element pcrf-dne2
```

### Configuring PCEF Profiles for Dynamic Policies

**CLI Quick Configuration** To quickly configure the PCEF profiles for dynamic policies, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge pcef profiles pcef-static-gx-offline-prof dynamic-policy-control]
set pcc-rules static-gx-offline-rule-1 precedence 10
set pcc-rules static-gx-offline-rule-2 precedence 50
set pcc-rules static-gx-offline-wildcard-rule precedence 1900
set diameter-profile gx1
[edit unified-edge pcef profiles pcef-static-gx-online-prof dynamic-policy-control]
```

```
set pcc-rules static-gx-online-rule-1 precedence 500
set pcc-rules static-gx-online-rule-2 precedence 510
set pcc-rules static-gx-online-wildcard-rule precedence 1950
set diameter-profile gx1
```

**Step-by-Step  
Procedure**

To configure dynamic PCEF profiles to enforce policy decisions that are received from the PCRF and provide the PCRF with subscriber and access information over the Gx interface:

1. Configure a dynamic PCEF profile to handle traffic for offline charging:

- a. Specify a name for the PCEF profile.

```
user@host# edit unified-edge pcef profiles pcef-static-gx-offline-prof
```

- b. Specify the application-aware PCC rules and rule precedence for the PCEF profile.

```
[edit unified-edge pcef profiles pcef-static-gx-offline-prof]
user@host# set dynamic-policy-control pcc-rules static-gx-offline-rule-1
precedence 10
user@host# set dynamic-policy-control pcc-rules static-gx-offline-rule-2
precedence 50
```

- c. Specify a wildcard PCC rule and precedence.

```
[edit unified-edge pcef profiles pcef-static-gx-offline-prof]
user@host# set dynamic-policy-control pcc-rules static-gx-offline-wildcard-rule
precedence 1900
```



**NOTE:** A PCEF profile that includes application-aware PCC rules must also include a wildcard Layer 3 or Layer 4 PCC rule at a lower precedence.

- d. Specify a diameter Gx profile for the PCEF profile.

```
[edit unified-edge pcef profiles pcef-static-gx-offline-prof]
user@host# edit dynamic-policy-control diameter-profile gx1
```

2. Configure a dynamic PCEF profile to handle online-charging traffic:

- a. Specify a name for the PCEF profile.

```
user@host# edit unified-edge pcef profiles pcef-static-gx-online-prof
```

- b. Specify the application-aware PCC rules and rule precedence for the PCEF profile.

```
[edit unified-edge pcef profiles pcef-static-gx-online-prof dynamic-policy-control]
user@host# set pcc-rules static-gx-online-rule-1 precedence 500
user@host# set pcc-rules static-gx-online-rule-2 precedence 510
```

- c. Specify a wildcard PCC rule and precedence.

```
[edit unified-edge pcef profiles pcef-static-gx-online-prof dynamic-policy-control]
user@host# set pcc-rules static-gx-online-wildcard-rule precedence 1950
```

- d. Specify a diameter Gx profile for the PCEF profile.

```
[edit unified-edge pcef profiles pcef-static-gx-online-prof dynamic-policy-control]
user@host# edit diameter-profile gx1
```

### Configuring PCEF Profiles for Static (Local) Services

**CLI Quick Configuration** To quickly configure a PCEF profile for static policies, copy the following commands and paste them into the router terminal window:

```
[edit unified-edge pcef profiles pcef-local-offline-prof]
set static-policy-control pcc-rules local-offline-rule-1 precedence 2001
set static-policy-control pcc-rules local-offline-rule-2 precedence 2010
set static-policy-control pcc-rules local-offline-wildcard-rule precedence 3900
set static-policy-control pcc-rulebases local-offline-rb-1
[edit unified-edge pcef profiles pcef-local-online-prof]
set static-policy-control pcc-rules local-online-rule-1 precedence 2500
set static-policy-control pcc-rules local-online-rule-2 precedence 2510
set static-policy-control pcc-rules local-online-wildcard-rule precedence 3950
set static-policy-control pcc-rulebases local-online-rb-1
[edit unified-edge pcef pcc-rules local-offline-rb-rule-1]
set from flows allow_all
set from applications junos:http
set from nested-applications junos:LINKEDIN
set then pcc-action-profile pap-4
[edit unified-edge pcef pcc-rules local-offline-rb-rule-2]
set from flows allow_all
set from applications junos:http
set from nested-applications junos:YAHOO-MAIL
set then pcc-action-profile pap-5
[edit unified-edge pcef pcc-rules local-online-rb-rule-1]
set from flows flow-tcp-1
set from applications junos:http
set from nested-applications junos:LINKEDIN
set then pcc-action-profile pap-14
[edit unified-edge pcef pcc-rules local-online-rb-rule-2]
set from flows flow-tcp-1
set from applications junos:http
set from nested-applications junos:YAHOO-MAIL
set then pcc-action-profile pap-15
[edit unified-edge pcef pcc-rulebases local-offline-rb-1]
set pcc-rule local-offline-rb-rule-1 precedence 3001
set local-offline-rb-1 pcc-rule local-offline-rb-rule-2 precedence 3010
[edit unified-edge pcef pcc-rulebases local-online-rb-1]
set pcc-rule local-online-rb-rule-1 precedence 3501
set pcc-rule local-online-rb-rule-2 precedence 3510
```

**Step-by-Step Procedure** To configure PCEF profiles for static (local) services:

1. Configure a local PCEF profile to handle traffic for offline charging:
  - a. Specify a name for the PCEF profile.
 

```
user@host# edit unified-edge pcef profiles pcef-local-offline-prof
```
  - b. Specify the application-aware PCC rules and rule precedence for the PCEF profile.
 

```
[edit unified-edge pcef profiles pcef-local-offline-prof]
```

```
user@host# set static-policy-control pcc-rules local-offline-rule-1 precedence
2001
user@host# set static-policy-control pcc-rules local-offline-rule-2 precedence
2010
```

- c. Specify a wildcard PCC rule and precedence.

```
[edit unified-edge pcef profiles pcef-local-offline-prof]
user@host# set static-policy-control pcc-rules local-offline-wildcard-rule
precedence 3900
```



**NOTE:** A PCEF profile that includes application-aware PCC rules must also include a wildcard Layer 3 or Layer 4 PCC rule at a lower precedence.

- d. Specify a rulebase for the PCEF profile.

```
[edit unified-edge pcef profiles pcef-local-offline-prof]
user@host# set static-policy-control pcc-rulebases local-offline-rb-1
set
set diameter-profile gx1
```

2. Configure a local PCEF profile to handle traffic for online charging:

- a. Specify a name for the PCEF profile.

```
[edit unified-edge pcef profiles pcef-local-online-prof]
set static-policy-control pcc-rules local-online-rule-1 precedence 2500
set static-policy-control pcc-rules local-online-rule-2 precedence 2510
set static-policy-control pcc-rules local-online-wildcard-rule precedence 3950
set static-policy-control pcc-rulebases local-online-rb-1

user@host# edit unified-edge pcef profiles pcef-local-online-prof
```

- b. Specify the application-aware PCC rules and rule precedence for the PCEF profile.

```
[edit unified-edge pcef profiles pcef-static-gx-online-prof static-policy-control]
user@host# set pcc-rules local-online-rule-1 precedence 2500
user@host# set static-policy-control pcc-rules local-online-rule-2 precedence
2510
```

- c. Specify a wildcard PCC rule and precedence.

```
[edit unified-edge pcef profiles pcef-static-gx-online-prof static-policy-control]
user@host# set static-policy-control pcc-rules local-online-wildcard-rule
precedence 3950
```

- d. Specify a rulebase for the PCEF profile.

```
[edit unified-edge pcef profiles pcef-static-gx-online-prof static-policy-control]
user@host# set static-policy-control pcc-rulebases local-online-rb-1
```

### Applying PCEF Policies for Dynamic Services to APNs

- CLI Quick Configuration** To quickly apply each PCEF profile to an access point name (APN), copy the following commands and paste them into the router terminal window:
- ```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-static-gx-offline]
set mobile-interface mif.0
set address-assignment allow-static-ip-address
set pcef-profile pcef-static-gx-offline-prof
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-static-gx-online]
set mobile-interface mif.1
set address-assignment allow-static-ip-address
set pcef-profile pcef-static-gx-online-prof
```
- Step-by-Step Procedure** To apply the dynamic PCEF policies to APNs:
1. Configure APNs to use for the MIF interfaces for the PCEF policies.
 

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-static-gx-online]
user@host# set mobile-interface mif.0
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-static-gx-offline]
user@host# set mobile-interface mif.1
```
  2. Configure the **allow-static-ip-address** address assignment for each APN so that the broadband gateway allows for a static IP address provided by the user equipment.
 

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-static-gx-online]
user@host# set address-assignment allow-static-ip-address
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-static-gx-offline]
user@host# set address-assignment allow-static-ip-address
```
  3. Configure APNs to use dynamic PCEF policies to use real-time analysis of the service to assign PCC rules.
 

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-static-gx-offline]
user@host# set pcef-profile pcef-static-gx-offline-prof
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-static-gx-online]
user@host# set pcef-profile pcef-static-gx-online-prof
```

### Applying a PCEF Profile for Static Services to an APN

- CLI Quick Configuration** To quickly apply the PCEF profile to an APN, copy the following commands and paste them into the router terminal window:
- ```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-local-offline]
set mobile-interface mif.0
set address-assignment allow-static-ip-address
set pcef-profile pcef-local-offline-prof
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-local-online]
set mobile-interface mif.1
set address-assignment allow-static-ip-address
set pcef-profile pcef-local-online-prof
```

- Step-by-Step Procedure** To apply the static PCEF policies to APNs:
1. Configure APNs to use for the MIF interfaces.

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-local-online]
user@host# set mobile-interface mif.0
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-local-offline]
user@host# set mobile-interface mif.1
```

2. Configure the **allow-static-ip-address** address assignment for each APN so that the broadband gateway allows for a static IP address provided by the user equipment.

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-local-online]
user@host# set address-assignment allow-static-ip-address
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-local-offline]
user@host# set address-assignment allow-static-ip-address
```

3. Configure APNs to use local PCEF policies to assign PCC rules.

```
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-local-offline]
user@host# set pcef-profile pcef-local-offline-prof
[edit unified-edge gateways ggsn-pgw PGW apn-services apns dpi-local-offline]
user@host# set pcef-profile pcef-local-online-prof
```

---

## Results

From configuration mode, confirm your configuration by entering the **show** command at the correct hierarchy level. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, this **show** command output includes only the configuration that is relevant to this example.

## Verification

To display Gx statistics and active bearer statistics to verify that the PCEF configuration on the broadband gateway is working properly, perform the following tasks:

- [Verifying Control Plane Gx Statistics on the Gateway on page 418](#)
- [Verifying Active Bearers on the Gateway on page 419](#)
- [Verifying Control Plane Gx Statistics on the Gateway on page 420](#)
- [Verifying Control Plane GX Statistics on the APN on page 420](#)
- [Verifying Application Identification Counter Statistics on page 423](#)
- [Verifying Application Signatures Counter Statistics on page 423](#)

---

### Verifying Control Plane Gx Statistics on the Gateway

**Purpose** Verify the control plane statistics for the Gx interface on the P-GW.



**Action** user@host> show unified-edge ggsn-pgw statistics

Gateway: PGW

Control plane GTP statistics:

|                                             |   |
|---------------------------------------------|---|
| Session establishment attempts:             | 6 |
| Successful session establishments:          | 6 |
| MS/peer initiated session deactivations:    | 4 |
| Successful MS/peer initiated deactivations: | 4 |
| Gateway initiated session deactivations:    | 0 |
| Successful gateway initiated deactivations: | 0 |

PCC Gx statistics:

|                                              |   |            |
|----------------------------------------------|---|------------|
| Session attempts using dynamic policy:       | 6 | Success: 6 |
| Dedicated bearer activation attempts:        | 5 | Success: 3 |
| MS-Peer init dedicated bearer deactivations: | 2 |            |
| Gateway init dedicated bearer deactivations: | 0 |            |
| PCRF init dedicated bearer deactivations:    | 0 |            |

Data plane global statistics:

|                                   |   |
|-----------------------------------|---|
| Source address violation packets: | 0 |
| Non-existent TEID/TID packets:    | 0 |
| GTP length error packets:         | 0 |
| Non-existent UE address packets:  | 0 |
| Mobile-to-mobile packets:         | 0 |

Data plane GTP statistics (Gn/S5/S8):

|                    |      |
|--------------------|------|
| Input packets:     | 15   |
| Input bytes:       | 1500 |
| Output packets:    | 15   |
| Output bytes:      | 1500 |
| Discarded packets: | 0    |

Data plane GTP statistics (Gi):

|                    |      |
|--------------------|------|
| Input packets:     | 15   |
| Input bytes:       | 1500 |
| Output packets:    | 15   |
| Output bytes:      | 1500 |
| Discarded packets: | 0    |

**Meaning** The `show unified-edge ggsn-pgw statistics` command displays all statistics at the gateway level for different interfaces.

### Verifying Active Bearers on the Gateway

**Purpose** Verify the active bearers on the P-GW.

**Action** user@host> show unified-edge ggsn-pgw status

Gateway: PGW

Mobile gateway status:

|                         |   |    |
|-------------------------|---|----|
| Active Subscribers      | : | 2  |
| Active Sessions         | : | 2  |
| Active Bearers          | : | 3  |
| Active GBR Bearers      | : | 1  |
| Active Non-GBR Bearers  | : | 2  |
| Active Prepaid bearers  | : | 0  |
| Active Postpaid bearers | : | 0  |
| CPU Load (%)            | : | 0  |
| Memory Load (%)         | : | 32 |

**Meaning** The `show unified-edge ggsn-pgw status` command displays the active subscribers, sessions, and bearers on the network.

### Verifying Control Plane Gx Statistics on the Gateway

---

**Purpose** Verify the control plane Gx statistics on the P-GW.

**Action**

```
user@host> show unified-edge ggsn-pgw statistics gateway PGW
Gateway: PGW
Control plane GTP statistics:
  Session establishment attempts:      6
  Successful session establishments:    6
  MS/peer initiated session deactivations: 4
  Successful MS/peer initiated deactivations: 4
  Gateway initiated session deactivations: 0
  Successful gateway initiated deactivations: 0
PCC Gx statistics:
  Session attempts using dynamic policy: 6      Success: 6
  Dedicated bearer activation attempts: 5      Success: 3
  MS-Peer init dedicated bearer deactivations: 2
  Gateway init dedicated bearer deactivations: 0
  PCRF init dedicated bearer deactivations: 0
Data plane global statistics:
  Source address violation packets:      0
  Non-existent TEID/TID packets:        0
  GTP length error packets:             0
  Non-existent UE address packets:      0
  Mobile-to-mobile packets:            0
Data plane GTP statistics (Gn/S5/S8):
  Input packets:                        15
  Input bytes:                         1500
  Output packets:                      15
  Output bytes:                        1500
  Discarded packets:                   0
Data plane GTP statistics (Gi):
  Input packets:                        15
  Input bytes:                         1500
  Output packets:                      15
  Output bytes:                        1500
  Discarded packets:                   0
```

**Meaning** The `show unified-edge ggsn-pgw statistics gateway PGW` command displays gateway-level statistics.

### Verifying Control Plane GX Statistics on the APN

---

**Purpose** Verify the control plane statistics for the Gx interface on the broadband gateway.

```

Action user@host> show unified-edge ggsn-pgw statistics gateway PGW apn apn-dynamic
Gateway: PGW
Control plane GTP statistics:
  Session establishment attempts:                21
  Successful session establishments:              20
  MS/peer initiated session deactivations:       12
  Successful MS/peer initiated deactivations:    12
  Gateway initiated session deactivations:       2
  Successful gateway initiated deactivations:    2
  MS initiated modification attempts:            0
  Successful MS initiated modifications:          0
  PGW/GGSN initiated modification attempts:      1
  Successful PGW/GGSN initiated modifications:   1
Redirect statistics:
  Successful apn redirects:                      0
  Attempted gateway redirects:                   0
  Successful gateway redirects:                  0
User authentication statistics:
  Authentication failures:                       0
  Attempted authentications:                     0
  Successful authentications:                    0
Address allocation statistics:
  Dynamic IP allocation attempts:                21
  Dynamic IP allocation success:                 21
Charging statistics:
  Number of CDRs allocated:                     25
  Number of partial CDRs allocated:              0
  Number of CDRs closed:                        17
  Number of containers closed:                   17
Static policy statistics:
  Session establishment attempts using static policy: 0
  Session establishment success using static policy: 0
DCCA-Gy Statistics:
  Online authorizations attempted:                0 Success : 0
  Online authorization timeouts:                  0
  Quota threshold reauthorization requests sent: 0
Gy Diameter msg statistics:
  CCR-Initial Sent : 0 Success : 0 Fail : 0
  CCR-Update Sent : 0 Success : 0 Fail : 0
  CCR-Terminate Sent : 0 Success : 0 Fail : 0
  RAR Received : 0 Answer : 0 Fail : 0
  ASR Received : 0 Answer : 0
  CCR Failure :
    Transient : 0
    Parameter : 0
    Permanent : 0
    Unknown code : 0
    Unknown session : 0
Session Establishments Failed (by GTP cause):
  Others 0
  Service unavailable: 0
  System failure: 0
  No resources: 0
  No address: 0
  Service denied: 0
  Authentication Fail: 0
  APN access denied: 0
PCC Gx statistics:
  Session attempts:                21 Success: 20
  MS-peer initiated APN-AMBR modification attempts: 0 Success: 0
  MS-peer initiated QoS modification attempts: 0 Success: 0

```

```

    PCRF initiated session deactivations:      0
    Gateway initiated session deactivations:    2
    MS-peer initiated session deactivations:    12
Gx modification statistics:
    Initiated by MS-peer: 0      Success: 0
    Initiated by PCRF:  8      Success: 0
Modification event reason:
    QoS change:      0      RAT change:      0
    SGSN change:     0      SGW change:     0
    PLMN change:     0      RAI change:     0
    ULI change:      0      IP-CAN change: 0
    TFT change (MS): 0      TFT change (Network): 0
    Bearer loss:     0      Bearer recovery:  0
    Resource allocation: 0    Revalidation Timeout: 0
    QoS exceeding auth: 0    Time-of-Day procedure: 0
    Change of Subscription: 0  AMBR change:      0
    ECGI change:     0      TAI change:      0
    Timezone change: 0      Default-EPS-QoS change:0
Dedicated bearer statistics:
    MS-peer initiated activation attempts: 0      Success: 0
    Network initiated activation attempts: 7      Success: 5
    MS-peer initiated modification attempts: 0     Success: 0
    Network initiated modification attempts: 0     Success: 0
    MS-peer initiated deactivations: 5
    Network initiated deactivations: 0
    Gateway initiated deactivations: 0
Gx Failure Statistics:
    GBR dedicated bearer create failure due to CAC: 0
    Non-GBR dedicated bearer create failure due to CAC: 0
    Session terminations due to unreachable PCRF: 0
    Session terminations due to PCRF restart: 0
Gx diameter message statistics:
    CCR-I sent: 21      CCA-I received: 20
    CCR-U sent: 20      CCA-U received: 20
    CCR-T sent: 15      CCA-T received: 0
    RAR received: 8      RAA sent: 6
    RAA sent resource failure: 0
CCR failure reason:
    Transient failure: 0      Initial params error: 0
    Permanent failure: 0     Unknown code: 0
    Unknown session: 0
Gx rule statistics:
    Dynamic rule activations: 0      Deactivations: 0
    Static rules activations: 10     Deactivations: 10
    Dynamic rule modifications: 20
Rule failure statistics:
    Rule validation failure: 14
    Rule enforcement failure no resource: 2
    Rule activation failure no resource: 0
    Rule update procedure fail: 0
Handover Statistics:
    Inter-RAT Handover attempts: 0      Success: 0
    Intra-RAT Handover attempts: 0      Success: 0
Data plane statistics:
    Total packets violating MIF ACL: 0
    Total accepted mobile-to-mobile packets: 0
    Total accepted mobile-to-mobile bytes: 0
Miscellaneous Packet statistics:
    IPv6 Router Solicitations received: 0
    IPv6 Router Advertisement transmitted: 0
    IPv6 Neighbor Solicitations received: 0

```

```

IPv6 Neighbor Advertisement transmitted:    0
Data plane GTP statistics (Gn/S5/S8):
  Input   packets:    0
  Input   bytes:      0
  Output  packets:    0
  Output  bytes:      0
  Discarded packets:  0
Data plane GTP statistics (Gi):
  Input   packets:    0
  Input   bytes:      0
  Output  packets:    0
  Output  bytes:      0
  Discarded packets:  0

```

**Meaning** The `show unified-edge ggsn-pgw statistics gateway PGW apn apn-dynamic` command displays the control plane Gx statistics for an APN. If the output shows that session attempts are successful, then the connection to the PCEF is functioning properly.

### Verifying Application Identification Counter Statistics

**Purpose** Verify the application identification (APPID) statistics on the broadband gateway.

**Action** `user@host> show services application-identification counter`

```

Counter Statistics:
  pic: ams1
  Total sessions: 78537
  Total identified sessions: 78537
  Total un-identified sessions: 0
  Protocol Method
    Total identified-by-protocol sessions: 0
    Total un-identified-by-protocol sessions: 0
  Address Method
    Total identified-by-address sessions: 0
    Total un-identified-by-address sessions: 78537
  Port Method
    Total identified-by-port sessions: 2053
    Total un-identified-by-port sessions: 0
    Total identified-by-icmp sessions: 0
    Total un-identified-by-icmp sessions: 0
    Total identified-by-ip-protocol sessions: 0
    Total un-identified-by-ip-protocol sessions: 0
  Signature Method
    Total identified-by-signature sessions: 76484
    Total identified-by-signature uni-directional sessions: 0
    Total un-identified-by-signature sessions: 2053
    Total unspecified encrypted sessions: 0
    Total encrypted P2P sessions detected by heuristics: 0
    Total application system cache hits: 0
    Total application system cache misses: 0

```

### Verifying Application Signatures Counter Statistics

**Purpose** Verify detailed information about a specified application signature, all application signatures, or a summary of the existing application signatures and nested application signatures. Both custom and predefined application signatures and nested application signatures can be displayed.

```
Action user@host> show services application-identification application detail junos:FACEBOOK-ACCESS
re0:
Application Name: junos:FACEBOOK-ACCESS
Application type: FACEBOOK-ACCESS
Description: This signature detects requests to Facebook.com, a social networking
Web site.
Application ID: 311
Disabled: No
Number of Parent Group(s): 1
Application Groups:
  junos:social-networking:facebook
Application Tags:
  characteristic      : Loss of Productivity
  characteristic      : Supports File Transfer
  characteristic      : Known Vulnerabilities
  characteristic      : Capable of Tunneling
  characteristic      : Can Leak Information
  risk                : 5
  subcategory          : Facebook
  category             : Social-Networking
Signature NestedApplication:FACEBOOK-ACCESS
Layer-7 Protocol: HTTP
Chain Order: Yes
Maximum Transactions: 20
Order: 33322
Member(s): 1
  Member 0
    Context: http-header-host
    Pattern: (.*\.)?(facebook\.com|fbcdn\.net)(:\d+)?
    Direction: CTS
```

## Troubleshooting

To troubleshoot the policy and charging enforcement function (PCEF) configuration, perform these tasks:

- [Connection Is Down Between the PCEF and PCRF on page 424](#)
- [PCEF and PCRF Application Messages Are Not Sent or Received on page 425](#)

---

### Connection Is Down Between the PCEF and PCRF

**Problem** The connection between the PCEF and PCRF peers on the Gx interface appears to be down.

**Solution** To display the Diameter peer status for the PCRF and PCEF:

1. From operational mode, enter the **show unified-edge ggsn-pgw diameter peer status** command.

```
user@host> show unified-edge ggsn-pgw diameter peer status
Gateway: PGW
Control plane GTP statistics:
  Session establishment attempts:          6
  Successful session establishments:        6
  MS/peer initiated session deactivations: 4
  Successful MS/peer initiated deactivations: 4
  Gateway initiated session deactivations: 0
```

```

    Successful gateway initiated deactivations: 0
PCC Gx statistics:
  Session attempts using dynamic policy:      6      Success: 6
  Dedicated bearer activation attempts:      5      Success: 3
  MS-Peer init dedicated bearer deactivations: 2
  Gateway init dedicated bearer deactivations: 0
  PCRF init dedicated bearer deactivations: 0
Data plane global statistics:
  Source address violation packets:          0
  Non-existent TEID/TID packets:            0
  GTP length error packets:                 0
  Non-existent UE address packets:          0
  Mobile-to-mobile packets:                0
Data plane GTP statistics (Gn/S5/S8):
  Input   packets:      15
  Input   bytes:       1500
  Output  packets:      15
  Output  bytes:       1500
  Discarded packets:    0
Data plane GTP statistics (Gi):
  Input   packets:      15
  Input   bytes:       1500
  Output  packets:      15
  Output  bytes:       1500
  Discarded packets:    0

```

2. Check that status of the State field, which is displayed at the beginning of the output. When the connection between the Diameter peers (PCEF and PCRF) is up, the State status indicates **I-Open**.
3. Check that the status of the Watchdog State field, which is displayed near the beginning of the output. When Diameter peers are connected, the Watchdog State status indicates **okay**.

### PCEF and PCRF Application Messages Are Not Sent or Received

**Problem** The PCRF and PCEF application messages (Re-Authorization Request/Re-Authorization Answer or Credit Control Request/Credit Control Answer) are not being sent or received.

**Solution** To display the status of application messages for the PCRF and PCEF:

1. From operational mode, enter the **show unified-edge ggsn-pgw diameter peer statistics** command.

```

user@host> show unified-edge ggsn-pgw diameter peer statistics
Peer: p1
Request Timeouts:          0
Request Retransmissions:  0
Messages                   Transmitted      Received
-----
Total Messages             22              22
Credit Control Requests   14              0
Credit Control Answers    0              14
Re-Auth Requests          0              2
Re-Auth Answers           2              0
Abort Session Requests    0              0
Abort Session Answers      0              0
Capability Exchange Requests 2              0

```

|                             |   |   |
|-----------------------------|---|---|
| Capability Exchange Answers | 0 | 2 |
| Device Watchdog Requests    | 4 | 0 |
| Device Watchdog Answers     | 0 | 4 |
| Disconnect Peer Requests    | 0 | 0 |
| Disconnect Peer Answers     | 0 | 0 |

2. Check that for each message type, there are an equal number of messages for requests and answers.

**Related  
Documentation**

- [Application-Aware Policy and Charging Control Rules Overview on page 353](#)
- [APPID Feature Overview on page 355](#)
- [Example: Configuring Policy and Charging Enforcement Function With Layer 3 and Layer 4 Policy and Charging Control Rules on page 379](#)



## PART 8

# Charging Configuration

- [Charging Overview on page 429](#)
- [Configuring Charging on page 443](#)



## CHAPTER 19

# Charging Overview

- [Charging Overview on page 429](#)
- [Offline Charging Overview on page 431](#)
- [Online Charging Overview on page 433](#)
- [Charging Data Records on page 434](#)
- [Charging Profiles on page 438](#)
- [Advice of Charge Overview on page 440](#)
- [Service Sets and Service Filters for Advice of Charge Overview on page 441](#)

## Charging Overview

---

Charging is an umbrella term that often covers not only charging, but also the rating and billing of services. Together, charging, rating and billing combine to assure that service providers are compensated by their customers or subscribers for the delivery of services.

More specifically, charging is used to describe the metering of services that are not free or are bundled in other ways with basic service features (such as handoffs). The opposite of a charge is a credit. Together, in the process called rating, charges and credits are applied to a subscriber's account to determine the periodic amount due to the service provider. If charges exceed credits, the subscriber's account is billed for a certain amount. Monthly telephony billing statements used to have a section called "other charges and credits" where these items were detailed, usually by date.

Charges can be determined by a number of different criteria, alone or in combination:

- Time (duration), often variable by time of day or distance between endpoints
- Pre-paid credits, which are consumed by users and often have a quota that can be exhausted
- Artificial units, which have no basis in reality, such as the old "message units" for telephony services

Charging rates can be set by contract or by public documents (called "tariffs") approved by a regulating entity. Tariffs and contract terms can vary by time of day, day of the week, or other intervals.

Service charges can be flat-rate or metered based on the various criteria outlined above. Flat-rate services are popular with customers (especially those on tight budgets), predictable, simple to maintain from an accounting perspective (few disputes arise over flat-rate services), and easy to bill. On the other hand, flat-rate services can deprive the service provider of additional revenues during periods of high usage and can result in forced expenses on the part of the subscriber during periods of low usage.

Metered services are popular with customers when services are inexpensive compared to other items in a budget, unpredictable, difficult to maintain from an accounting perspective (many disputes arise over metered services), and more complex to bill. However, in contrast to flat-rate services, metered services provide additional revenues when resource use is high (due to a suddenly popular service), spreading the financial burden among customers based on actual usage.

The accrued amount of subscriber charges can be conveyed to the subscriber in real time as they occur, periodically (monthly bills were a common feature in telephony), or on request. The use of one main method need not preclude the others.

## Charging in Mobile Networks

In the mobile network, it is important to have detailed and accurate monitoring of service usage on the MobileNext Broadband Gateway so that proper charging information can be generated for millions of customers. In the Third-Generation Partnership Project (3GPP), there are three distinct aspects to the process that translates service use into a bill for services. These aspects are charging, rating, and billing. Charging gathers statistics about service usage for each customer. Rating is the process of determining how much each service costs each particular customer, based on the services contracted or tariffed. Billing is the process of actually generating the customer's invoice for services.

The MobileNext Broadband Gateway is the anchor of the data call and contains most of the subscriber context information. The broadband gateway is responsible for collecting charging information related to the external data network usage and to network resource usage on the Gateway GPRS Support Node (GGSN) or Packet Data Network Gateway (P-GW), including the amount of data categorized by quality of service (QoS), the user protocols, and the usage of the packet data protocol address. Packet data volume in both the uplink (from the Gn-to-Gi interface) and downlink (from the Gi-to-Gn interface) directions is counted separately.

Long Term Evolution (LTE) mobile networks define two different types of charging systems: Offline Charging Systems (OFCS) and Online Charging Systems (OCS). Offline charging is usually used for post-paid services for which the subscriber receives a bill (typically monthly). Online charging is well suited for pre-paid services. Online charging can affect a session in real time. For example, a session can be terminated if the subscriber runs out of credit. Offline charging cannot affect subscribers in real time. Typically, a service provider will provision both offline and online charging for subscribers.

## Charging with Data Records (Offline Charging)

In offline charging, a charging trigger monitors the subscriber's use of services and resources and generates charging events that describe the system charge activities. A charging data function, which can be integrated with the gateway device, processes

charging events and collects these as Charging Data Records (CDRs). The CDRs are written to files or transferred to the OFCS charging gateway over the Ga interface using the GPRS Tunneling Protocol (GTP) prime (GTPP) protocol. The billing domain determines the cost of the resources used and invoices the subscriber.

If the user is roaming, the billing domain and charging gateway are in the subscriber's home network, while the charging data function is in the same network as the Serving Gateway (S-GW) and Packet Data Network Gateway (P-GW). The visited network also uses the roaming CDRs to invoice the home network for the roaming subscriber's use of visited resources (a process called settlement).

## Charging in Real Time (Online Charging)

In online charging, a charging trigger in the P-GW sends a credit request to the online charging function over the Gy interface to see if a session can begin. A rating function determines the subscriber's balance and replies with a credit authorization (which usually also specifies how long the session can last or how much data can be transferred). The charging trigger monitors the session and use of resources. If the allocation nears its limit, another credit request is sent for additional resources. When the session is over, the charging trigger notifies the OCS with regard to any remaining credit to return to the subscriber.

If the user is roaming, the OCS is always in the subscriber's home network. As in offline charging, the visited network uses the roaming CDRs to invoice the home network for the roaming subscriber's use of visited resources (settlement).

### Related Documentation

- [Offline Charging Overview on page 431](#)
- [Online Charging Overview on page 433](#)
- [Configuring GTP Prime for Charging on page 453](#)
- [Configuring Persistent Storage on page 455](#)
- [Charging Data Records on page 434](#)
- [Charging Profiles on page 438](#)
- [Example: Configuring Online Charging on page 486](#)

## Offline Charging Overview

The MobileNext Broadband Gateway supports offline charging, which is commonly used in a postpaid environment. The broadband gateway provides mobile operators with an intelligent charging service that has flexible provisioning and accurate resource usage record collection for their mobile subscribers. The broadband gateway gathers Charging Data Records (CDRs) and delivers them to the charging gateway function (CGF) over the Ga interface using the GTP Prime protocol. The billing function is distributed across all modules of the broadband gateway, which performs these tasks for billing:

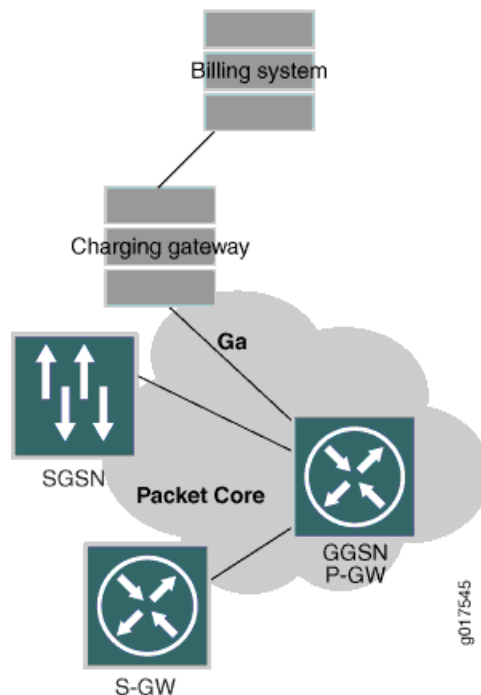
- Accurate CDR creation and closure
- Partial record generation

- ASN.1 or 3GPP formatting of CDRs prior to transfer to CGF or local storage
- Support of GTP Prime protocol stack to transfer CDRs to the CGF
- Support of primary, secondary, and tertiary CGF for redundancy of each charging profile

Charging information collection does not affect real-time operations and is transferred over the Ga interface using the GTP Prime protocol. The network element generates the CDR for each subscriber and reports it periodically to the charging gateway. The charging gateway then optionally reformats and transfers the collected CDRs to the operator's billing system for billing purposes.

Figure 53 on page 432 shows the components in a sample charging topology.

### Figure 53: Simple Charging Topology



The provisioning of the charging services follows this process:

1. Configure the CGF or local storage.
2. Create the transport profile and associate the primary, secondary, and tertiary CGF.
3. (Optional) Configure the CDR and trigger profiles.
4. Create a charging profile with a profile ID and the associated transport, CDR, and trigger profiles. The profile ID is used to match against the charging characteristic information element sent in the GTP create request or the RADIUS profile ID attribute-value pairs (AVPs) from the RADIUS authentication response.
5. In the access point name (APN) configuration, configure the charging profile selection order as static to select locally configured charging profiles.

The binding of the charging services, as well as the charging information collection, follows this process:

1. The broadband gateway starts to establish a bearer when the broadband gateway receives the request from the mobile subscriber to create a packet data protocol (PDP) context.
2. For each new bearer created in the broadband gateway, the configured charging profile selection order algorithm is applied and a charging profile is associated with the bearer.
3. The broadband gateway generates a container or CDR for every trigger or signaling event that the operator wants reported for this subscriber.
4. When the mobile subscriber terminates the session, the final network usage is reported to the CGF by the broadband gateway.

**Related  
Documentation**

- [Charging Overview on page 429](#)
- [Online Charging Overview on page 433](#)
- [Configuring GTP Prime for Charging on page 453](#)
- [Configuring Persistent Storage on page 455](#)
- [Charging Data Records on page 434](#)
- [Charging Profiles on page 438](#)
- [Example: Configuring Online Charging on page 486](#)

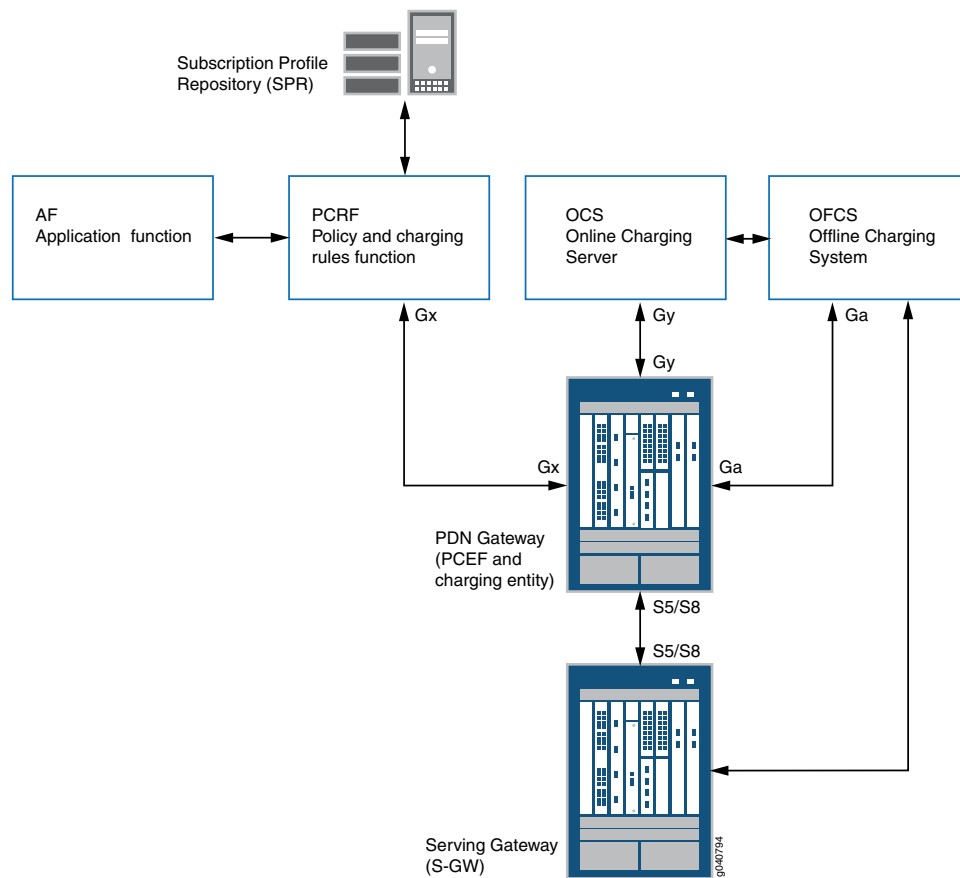
---

## Online Charging Overview

Online charging is part of a complete MobileNext Broadband Gateway configuration, including policy and charging rules, quality-of-service (QoS) determination, and overall charging considerations. The Gy interface connects the Packet Data Network Gateway (P-GW) and Online Charging System (OCS).

The unique aspect of online charging is that charging information can affect the subscriber's access to service in real time. The OCS delivers information to the P-GW that is used to control credits. Events that are of interest to online charging include bearer resource usage, especially data services. Data usage information is converted to charging events which are sent to the OCS, where available credit and rating is used to determine service access parameters. The OCS can deny use of the resource when credits are low, often by terminating the call. [Figure 54 on page 434](#) shows the overall architecture for the gateway components and the functional groupings for policy and charging.

Figure 54: General Architecture for Charging



The Gy interface between P-GW and OCS uses the Diameter protocol.

#### Related Documentation

- [Charging Overview on page 429](#)
- [Offline Charging Overview on page 431](#)
- [Configuring GTP Prime for Charging on page 453](#)
- [Configuring Persistent Storage on page 455](#)
- [Charging Data Records on page 434](#)
- [Charging Profiles on page 438](#)
- [Example: Configuring Online Charging on page 486](#)

## Charging Data Records

The MobileNext Broadband Gateway gathers charging information in Charging Data Records (CDRs). The broadband gateway supports different charging format versions.



The broadband gateway generates CDRs that contain the following types of information to charge a mobile station user or subscriber for accessing data from access point name (APN) networks:

- Data volume—Amount of data sent to and received from the APN networks.
- Duration of packet data protocol (PDP) context—Length of PDP context or call.
- Quality-of-service (QoS) classes—Priority at which requested data is transported.
- Roaming—Charges imposed for subscriber roaming among SGSNs belonging to a mobile operator or between different mobile operators.
- Tariff—Charges imposed based on the time of day.

CDRs can be delivered by the following methods:

- CDRs are transferred directly to a charging gateway server using the GTP Prime protocol.

The GTP Prime protocol supports UDP or TCP as the transport protocol, and IPv4 addresses. You must configure the charging gateways as GTP Prime peers. The peers can be configured for use by transport profiles as primary, secondary, or tertiary servers.

The broadband gateway supports sending the following messages:

- Node Alive Response—Response to a Node Alive Request received from the charging gateway function (CGF). The Node Alive Request message is used to indicate that a node in the network has started its service.
- Echo Request and Echo Response—The Echo Request message detects the path status between the CGF and the broadband gateway and should not be sent more than once every 60 seconds using UDP as the transport protocol.
- Redirect Request—CGF can send Redirect Request messages to the broadband gateway to advise that received CDR traffic is to be redirected to another CGF or that the next node in the chain (such as a mediation device or billing computer) has lost its connection to the CGF. When the request is to redirect to another CGF, the transport profile switches to the recommended CGF only if it is configured as a peer in the transport profile; otherwise, it switches to the next highest-priority peer in the transport profile.
- CDRs are logged to the local persistent storage and eventually retrieved by a charging gateway using the File Transfer Protocol (FTP). In broadband gateways configured with a backup Routing Engine, a mirror directory of CDRs is available.

Local persistent storage stores the CDRs in the form of files on the Routing Engine. When the transport profile is configured to use local persistent storage for CDRs, the session DPC sends the CDRs to the Routing Engine as temporary log files. When the triggers (such as file age, file size, or CDR count) acting on the temporary log files are reached, the temporary log file is closed and moved to the final log directory where it is available for transfer by the operator. By default, the configured user or root user is authorized to access the files. However, you can configure the log files to be readable by all users.

The final CDR log files are stored in the `/opt/mobility/charging/ggsn/final_log` directory in the filename format ***NodeID\_-PIC\_-transport-profile-id\_-RC.date\_-time[.PI].cdr***, where:

- *NodeID*—Name of the host that generated the file.
- *PIC*—The PIC number generating the CDR.
- *transport-profile-id*—The number of the transport profile generating the CDR.
- *RC*—Running count or sequence number, starting with the value of 1.
- *date*—Date when the CDR file was closed in the format *YYYYMMDD*, where *YYYY* is the year, *MM* is the month (01-12), and *DD* is the day (01-31).
- *time*—Time when the CDR file was closed in the format *HHMMshhmm*, where *HH* is the local time hour of day (00-23), *MM* is the local time minute of the hour (00-59), *s* is the sign of local time differential from UTC (+ or -), *hh* is the local time differential hour (00-23), and *mm* is the local time differential minute (00-59).
- *PI*—(Optional) Private information that is explicitly configured.
- *cdr*—File extension is always *cdr*.

For example, a final CDR log file could be named  
**magnet-PGW-1-3\_-\_155970.20120612\_-\_0950-0700.asn.cdr.**

The charging gateway consolidates charges for a particular PDP context from the broadband gateway. Each CDR is marked with a charging ID that identifies the mobile station user and the particular PDP session. This charging ID correlates information generated by the broadband gateway. Each CDR also includes a Local Record Sequence Number (LRSN) that is allocated sequentially and is unique for each CDR on the same session DPC. The LRSN is the IP address of the broadband gateway and the node ID. The charging gateway uses the LRSN to identify missing records. The billing gateway uses the charging ID and the LRSN to identify CDRs. The billing gateway server generates the information used in the bill that is sent to the subscriber.

## Information Collection and CDR Generation

Upon establishment of a PDP context, the broadband gateway opens a first partial CDR if it is configured to generate CDRs for the PDP context. The broadband gateway generates this CDR in Abstract Syntax Notation 1 (ASN.1) format. This format provides a common syntax for data transmitted between different communication systems.

This partial CDR contains static and dynamic information. The static information includes details such as the type of record (in this case, a CDR) and the international mobile station identifier (IMSI) of the subscriber. Additional information included in the CDR is based on the dynamic usage of an APN network by the subscriber. To collect dynamic usage information, the broadband gateway monitors the uplink and downlink bearer traffic associated with a PDP context.

A container holds the incremental statistics for the bearer. Each CDR has the containers that belong to the same bearer. Depending on the event, a container can be added to the CDR. You can configure the maximum number of containers for the CDR. Upon reaching this limit, the CDR is closed and sent to the CGF. The broadband gateway adds a container to the partial CDR each time one of the following chargeable events occurs:

- The QoS changes.
- The tariff changes.
- Other charging conditions are satisfied.

For example, if the QoS changes, a container is added. If the tariff changes, another container is added. If the QoS changes again, another container is added and so on until the maximum number of containers is reached.

The broadband gateway adds a container to the partial CDR and closes the CDR when one of the following chargeable events occurs:

- The PDP context terminates.
- The time limits are exceeded.
- The volume limits are exceeded.

The broadband gateway closes a partial CDR and opens a subsequent partial CDR if one of the following occurs:

- The configured number of containers for the container limit attribute is reached.
- A configurable data volume limit for the first partial CDR is reached. Each container has a data volume count associated with the chargeable event. Initially, the first partial CDR contains one container with 0 bytes of data volume.
- A configurable time limit for the first partial CDR is reached.
- The maximum of five SGSN or S-GW changes is reached. A container can include a list of up to five changes.

A very active broadband gateway has to generate a large number of CDRs. Many CDRs contain a lot of information that is not necessary for a given PDP context or is known to the charging gateway by other means. To minimize the size of the generated CDR packets, the charging configuration contains a variety of CDR attributes that can be excluded from CDRs if the information is not necessary.

After a PDP context terminates, a broadband gateway adds a container to the current partial CDR, closes it, and delivers it to a charging gateway using the configured CDR delivery method.

## CDR Delivery

CDR delivery to a charging gateway is based on the transport profile configuration. You can configure primary, secondary, and tertiary external charging gateways or local persistent storage in the transport profile. You must configure either the external charging gateways or local persistent storage, or both.

To support high throughput, the distributed control plane modules on the broadband gateway independently send CDRs to the charging gateway through their own UDP/TCP communication path. However, connectivity to the charging gateway is fate-shared. Thus, when one control plane reports loss of connectivity, all control planes switch to the next charging gateway in the peer order. This behavior also applies to GTP Prime echo failure, node alive, and redirect messages. The redirect message can contain the recommended charging gateway to switch to, but the transport profile switches to this charging gateway only if it is configured in the transport profile. Otherwise, it is redirected to the next higher-priority charging gateway in the peer order.

If the broadband gateway loses connectivity to all the charging gateways or the charging gateway is too slow, each control plane has a staging area to temporarily prevent the loss of CDRs. To prevent CDR and charging container record loss, all records are backed up to the backup control plane if redundancy is configured.

**Related  
Documentation**

- [Charging Overview on page 429](#)
- [Offline Charging Overview on page 431](#)
- [Online Charging Overview on page 433](#)
- [Configuring Offline Charging on page 443](#)
- [Configuring Transport Profiles for Offline Charging on page 459](#)
- [Example: Configuring Online Charging on page 486](#)

---

## Charging Profiles

The broadband gateway associates a charging profile with a mobile subscriber when a bearer is established. The charging profile specifies the charging behavior to apply based on the subscriber's charging characteristics. The charging behavior includes the charging mechanism, charging information sets, and charging transport behavior. The charging behavior depends on the charging type (for example, charging gateway or RADIUS server) and the associated charging profile.

Charging profiles can reference these profiles, which define the charging behavior:

- CDR profile—Defines the attributes in each CDR transmitted to the charging gateway.  
You can enable the generation of reduced partial CDRs and configure the exclusion of information elements from the CDR.
- Transport profile—Defines how to transfer the CDR to the charging gateway.  
You can specify information about the CDRs, including CDR format and aggregation limit, being transferred to the charging gateways. You can specify the order of the charging gateways.
- Trigger profile—Defines the effective charging events that trigger CDR creation and container addition or closure.

You can specify triggers, including:

- Time limits—Maximum age of collected charging data before a subsequent CDR is generated.
- Volume limits—Maximum amount of collected charging data before a subsequent CDR is generated.
- Tariff activation times—Time windows in which tariffs change for charging purposes. If the services provided by an APN network have different time windows and tariffs, you can configure the broadband gateway to update CDRs when the tariffs change.
- Container limits—Maximum number of containers in each CDR before a subsequent CDR is generated.
- Bearer changes—Bearer information changes to ignore for charging data updates. Charging updates are not triggered by changes to this information.

## Charging Profile Selection Process

The MobileNext Broadband Gateway has a highly flexible charging profile selection algorithm that enables the operator to choose the appropriate charging configuration for each subscriber. Provisioning is done for each APN, where the operator can specify the profile selection order for the charging profile.

You can specify that the charging profile be selected from the following sources in the preferred order:

- Subscriber type (static)—Use the configured charging profile for the type of subscriber (home, roamer, or visitor). If the charging profile for the type of subscriber is not configured for the APN, then the default profile is used if configured.
- SGSN or Serving Gateway (serving)—Use the charging profile sent by the SGSN or Serving Gateway.
- RADIUS server (radius)—Use the charging profile provided by the RADIUS server.

If the charging profile cannot be selected from the first source in the profile selection order, then the algorithm will try the next source. If no charging profile can be selected from any source, then charging is disabled for the subscriber.

### Related Documentation

- [Charging Overview on page 429](#)
- [Configuring Offline Charging on page 443](#)
- [Configuring Charging Profiles on page 467](#)
- [Configuring Transport Profiles for Offline Charging on page 459](#)
- [Configuring Charging Trigger Events for Offline Charging on page 462](#)
- [Configuring CDR Attributes on page 464](#)
- [Configuring Charging Profiles for APNs on page 469](#)
- [Example: Configuring Online Charging on page 486](#)

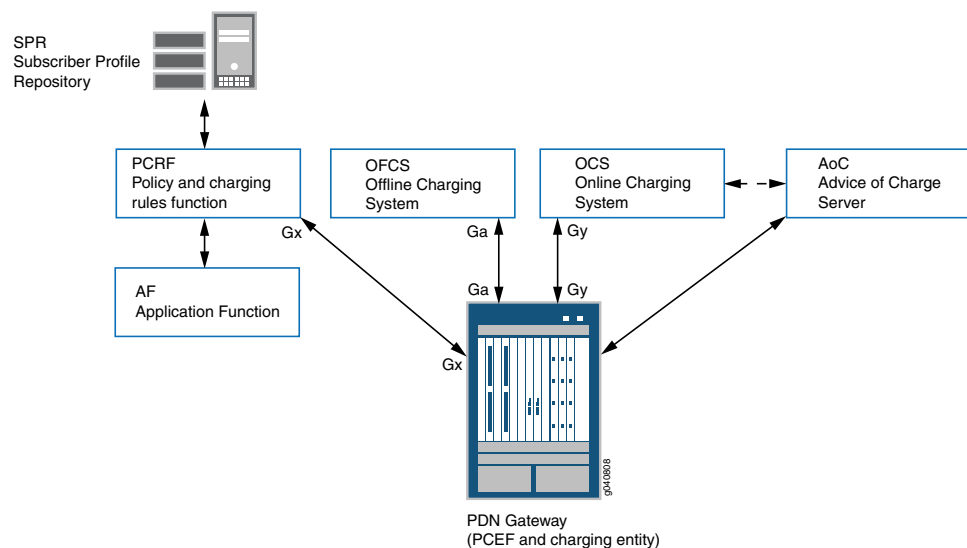
## Advice of Charge Overview

The Advice of Charge (AoC) feature provides a subscriber with information about any applicable charges when the subscriber uses a service. AoC information is provided *before* the subscriber uses the service, and the subscriber must accept the charges in order to use the service. This is in contrast with typical charging scenarios where subscribers who use a service are provided information about any charges only *after* they have used the service.

For prepaid subscribers, the charges are applied in real time until the subscriber's quota is exhausted. The subscriber is then given the opportunity to recharge; this is called Top-Up.

The MobileNext Broadband Gateway configured as a Gateway GPRS Support Node (GGSN) or Packet Data Network Gateway (P-GW) can be configured to provide AoC information to subscribers. Currently, AoC and Top-Up are provided for prepaid subscribers. [Figure 55 on page 440](#) displays the overall architecture for the gateway components and the functional groupings for AoC and Top-Up.

**Figure 55: System Architecture for Advice of Charge and Top-Up**



This topic includes the following sections:

- [Advice of Charge on the Broadband Gateway on page 440](#)

## Advice of Charge on the Broadband Gateway

The broadband gateway provides AoC and Top-Up features using HTTP redirection. The subscriber HTTP traffic is redirected to an AoC or Top-Up server based on triggers provided by the Online Charging System (OCS). HTTP traffic is redirected for one of the following reasons:

- The OCS must notify subscribers who request a new service about the charges.

- The OCS must notify subscribers of tariff changes when they roam in a foreign public land mobile network (PLMN).
- The OCS has sent the final unit indication with the action set to redirect and the subscriber runs out of quota.

The following is a high-level overview of the AoC process:

1. The subscriber who is using online charging connects to or roams into a new PLMN.
2. The broadband gateway sends a Credit Control Request (CCR) message to the OCS.
3. The OCS analyzes the information in the CCR message and determines that the subscriber must be redirected.
4. The OCS requests redirection by sending the appropriate information in the Credit Control Answer (CCA) message.
5. The broadband gateway sends the redirect URL (constructed from the information in the CCA message) to the subscriber's user equipment (UE).
6. The user equipment connects to the redirect URL and the broadband gateway forwards the request to the AoC or Top-Up server.
7. The AoC or Top-Up server sends a response to user equipment and provides information about new tariff plans and recharge options.
8. The subscriber tops up (recharges) or agrees to the tariff.
9. The AoC or Top-Up server informs the OCS about the acceptance charges or the top-up.
10. The subscriber continues the browsing session, with the broadband gateway forwarding the requests.

**Related Documentation**

- [Configuring Service Sets and Service Filters for Advice of Charge on page 495](#)
- [Service Sets and Service Filters for Advice of Charge Overview on page 441](#)

## Service Sets and Service Filters for Advice of Charge Overview

The Advice of Charge (AoC) feature provides a subscriber with information about any applicable charges *before* the subscriber uses a service, or when the subscriber's quota is exhausted. This intervention is provided by “filtering” or sifting the packet traffic to find those requiring AoC treatment. The AoC feature parameters are configured in several places that all come together in a firewall filter and a service set attached to the mobile interface (mif) of an access point name (APN) for input and output traffic. For AoC purposes, you apply the AoC service set and filter to input and output traffic. The service set and service filter names are variables, but must conform to the usual Junos OS naming rules.

The broadband gateway finds traffic packets that require AoC notification and sends the packets to a services interface (usually an aggregated multiservices [ams-] interface).

The services PIC forwards the information to the AoC server and then relays the reply to the user device.

In addition to the service set, firewall service filter, and mobile interface configuration, the AoC feature requires the configuration of a zero-rated or unlimited rating group (RG) to redirect traffic towards the AOC and top-up server for recharge when the subscriber quota is exhausted.

Therefore, several individual configurations all come together when the AoC feature is applied to the mobile interface:

- The policy and charging enforcement function (PCEF) profile configured at the **[edit services pcef profile]** hierarchy level. This profile must be referenced in the AoC service set configured at the **[edit services service-set]** hierarchy level.
- The AoC service filter configured at the **[edit firewall family inet service-filter aoc-filter-name]** hierarchy level. This filter sifts through the packet flow to detect those needing AoC.
- The service set and service filters applied to the mobile interface (mif) configured at the **[edit interfaces mif]** hierarchy level. The service sets and service filters are applied to input and output traffic.
- The Policy and Charging Control (PCC) action profile configuration to create a zero-rated rating group, and the PCC rule configuration to create a zero-rated flow that references the configured PCC action profile.

All four must be configured properly in order for AoC to function as intended.

**Related  
Documentation**

- [Advice of Charge Overview on page 440](#)
- [Configuring Service Sets and Service Filters for Advice of Charge on page 495](#)
- [Configuring Policy and Charging Control Action Profiles on page 369](#)
- [Configuring Application-Aware Policy and Charging Control Rules on page 371](#)



## CHAPTER 20

# Configuring Charging

- [Configuring Offline Charging on page 443](#)
- [Configuring S-GW-Specific Charging Parameters on page 444](#)
- [Configuring S-GW Global Charging Profiles and Selection Order on page 446](#)
- [Configuring S-GW Charging Traceoptions on page 448](#)
- [Configuring S-GW Local Persistent Storage Traceoptions on page 451](#)
- [Configuring GTP Prime for Charging on page 453](#)
- [Configuring Persistent Storage on page 455](#)
- [Configuring the Solid State Disk for Persistent Storage on page 457](#)
- [Configuring Transport Profiles for Offline Charging on page 459](#)
- [Configuring Charging Trigger Events for Offline Charging on page 462](#)
- [Configuring CDR Attributes on page 464](#)
- [Configuring Charging Profiles on page 467](#)
- [Configuring Charging Profiles for APNs on page 469](#)
- [Tracing Charging Operations on page 470](#)
- [Configuring Online Charging on page 472](#)
- [Configuring Transport Profiles for Online Charging on page 473](#)
- [Configuring Charging Trigger Events for Online Charging on page 476](#)
- [Verifying and Managing the Charging Configuration on page 484](#)
- [Example: Configuring Online Charging on page 486](#)
- [Configuring Service Sets and Service Filters for Advice of Charge on page 495](#)

## Configuring Offline Charging

---

You can configure the charging function on the MobileNext Broadband Gateway. The broadband gateway supports the configuration of offline charging. Offline charging can be configured to send Charging Data Records (CDRs) to charging gateways, to store CDRs on local physical storage, or both.

To configure the broadband gateway for offline charging:

- Configure the GPRS tunneling protocol (GTP) Prime properties for transmitting the CDR to the external charging gateway.

You must perform this task if you are using an external charging gateway. You can also configure the local persistent storage options to store CDRs on the Routing Engine.

- Configure the local persistent storage options on the Routing Engine for the CDRs.

You must perform this task if you want to configure offline charging and do not configure an external charging gateway.

- Configure the transport profile, which specifies information about the CDRs being transferred to the specified charging gateways, including the CDR format and aggregation limit.
- (Optional) Configure the trigger profile, which specifies the charging events that trigger the creation of the CDR or the addition or closure of the container.
- (Optional) Configure the CDR profile, which specifies the attributes in each transmitted CDR.
- Configure the charging profile, which specifies the charging behavior to apply based on profiles included in the charging profile. The included profiles must be defined.
- Configure the charging profiles for the access point names (APNs).
- Configure tracing for charging operations.

**Related  
Documentation**

- [Configuring GTP Prime for Transferring CDRs on page 453](#)
- [Configuring Persistent Storage on page 455](#)
- [Configuring Transport Profiles for Offline Charging on page 459](#)
- [Configuring Charging Trigger Events for Offline Charging on page 462](#)
- [Configuring CDR Attributes on page 464](#)
- [Configuring Charging Profiles on page 467](#)
- [Configuring Charging Profiles for APNs on page 469](#)
- [Tracing Charging Operations on page 470](#)
- [Charging Data Records on page 434](#)

---

## Configuring S-GW-Specific Charging Parameters

The MobileNext Broadband Gateway Serving Gateway (S-GW) uses three charging statements unique to the S-GW. This topic shows how to configure the charging statements that are unique to the S-GW.

Before you begin configuring S-GW charging parameters on the broadband gateway, you should have done the following:

- Configured the chassis of the MobileNext Broadband Gateway

- Configured the interfaces used by the MobileNext Broadband Gateway

To establish the charging parameters unique to the S-GW, you can exclude certain trigger events and specific charging detail record (CDR) information. The use of all three statements is optional.

To configure the S-GW charging parameters trigger profile exclusion:

1. (Option) Configure the S-GW charging trigger profile change exclusion.

```
[edit unified-edge gateways sgw MBG-SGW1 charging trigger-profiles TP1 offline
exclude-attributes]
user@host# set sgsn-mme-change
```



**NOTE:** When this statement is configured, a change in Serving GPRS Support Node (SGSN) or S-GW does not generate a charging data update.

2. (Option) Exclude the P-GW address used in the CDR attribute.

```
[edit unified-edge gateways sgw MBG-SGW1 charging cdr-profiles CDR1
exclude-attributes]
user@host# set pgw-address-used
```



**NOTE:** When this statement is configured, the P-GW IP address is not included in the CDR.

3. (Option) Exclude the S-GW change from the CDR attribute.

```
[edit unified-edge gateways sgw MBG-SGW1 charging cdr-profiles CDR1
exclude-attributes]
user@host# set sgw-change
```



**NOTE:** When this statement is configured, the S-GW change attribute is not included in the CDR.

4. Configure the CDR release.

```
[edit unified-edge gateways sgw MBG-SGW1 charging transport-profiles
MBG-SGW1-T-Profile offline charging-gateways]
user@host# set cdr-release r8
```



**NOTE:** By default, the S-GW supports Release 8. You must include this statement to change the supported release.

#### Related Documentation

- [Configuring Offline Charging on page 443](#)
- [Configuring S-GW Global Charging Profiles and Selection Order on page 446](#)
- [Configuring S-GW Charging Traceoptions on page 448](#)

- [Configuring S-GW Local Persistent Storage Traceoptions on page 451](#)
- [Configuring GTP Prime for Transferring CDRs on page 453](#)
- [Configuring Persistent Storage on page 455](#)
- [Configuring Transport Profiles for Offline Charging on page 459](#)
- [Configuring Charging Trigger Events for Offline Charging on page 462](#)
- [Configuring CDR Attributes on page 464](#)
- [Configuring Charging Profiles on page 467](#)
- [Configuring Charging Profiles for APNs on page 469](#)
- [Tracing Charging Operations on page 470](#)
- [Charging Data Records on page 434](#)

---

## Configuring S-GW Global Charging Profiles and Selection Order

The MobileNext Broadband Gateway Serving Gateway (S-GW) uses five global profiles for charging. This topic describes the profiles and shows how to configure the profile statements unique to the S-GW.

Before you begin configuring a S-GW CAC parameters on the broadband gateway, you should have done the following:

- Configured the chassis of the MobileNext Broadband Gateway
- Configured the interfaces used by the MobileNext Broadband Gateway
- Configured the charging profiles used by the MobileNext broadband Gateway

Global charging profile configuration is a mandatory configuration to enable charging on the S-GW. Configuring the **profile-selection-order** statement is mandatory when the **global-profile** statement is configured. The S-GW determines the type of subscriber by comparing the mobile country code (MCC) and the mobile network code (MNC) values in the Create Session Request message from the subscriber's user equipment (UE) with the corresponding values configured for the home public land mobile network (HPLMN) for the S-GW. Depending on whether a subscriber is a home subscriber, a visitor, or a roamer, the **home-profile**, **visitor-profile**, or **roamer-profile** is applied. If the applicable profile is not configured, then the **default-profile**, if configured, is applied. If the **default-profile** is not configured, then no charging is applied to the subscriber session.



**NOTE:** The profiles must already be configured on the broadband gateway before you reference them in the profile statements.

---

The default profile is applied if other profiles are absent. If the **profile-selection-order** configuration is **static**, and if the corresponding charging profile applicable to the type of subscriber (home, visitor, or roamer) has not been specified, then the default profile is applied.

The home profile is applied to home users based on the PLMN configuration. If the **profile-selection-order** configuration is **static**, and this is a home user, then the home profile is applied.

The roamer profile is applied to roaming users based on the PLMN configuration. If the **profile-selection-order** configuration is **static**, and this is a roaming user, then the roaming profile is applied.

The visitor profile is applied to visiting users based on the PLMN configuration. If the **profile-selection-order** configuration is **static**, and this is a visiting user, then the visiting profile is applied.

The profile selection order determines the order that the methods used to select a charging profile are applied. You can specify up to three profile selection methods: **static**, **serving**, or **pgw-cg-addr**. If the first choice is not available, then the next choice is considered, and so on.



**NOTE:** If no charging profile can be selected for the user, then the subscriber is not charged for the session.

Consider a configured profile selection order of **static**, **serving**, and **pgw-cg-addr**. Because **static** is the first choice, the global charging profiles specified are used. If the global charging profiles are not configured, then the next choice (**serving**) is considered. If the Serving GPRS Support Node (SGSN) or S-GW does not provide a charging profile identifier in the charging characteristics information element (IE) within the GPRS tunneling protocol (GTP) Create Session message, then the next choice (**pgw-cg-addr**) is considered. With the **pgw-cg-addr** option, the global charging profile is selected based on the IP address of the charging gateway (CG) for the P-GW.

To configure the S-GW global charging profiles and selection order:

1. Configure the S-GW default global charging profile.

```
[edit unified-edge gateways sgw MBG-SGW1 charging global-profile]
user@host# set default-profile MBG-SGW1-default
```

2. Configure the S-GW home user global charging profile.

```
[edit unified-edge gateways sgw MBG-SGW1 charging global-profile]
user@host# set home-profile MBG-SGW1-home
```

3. Configure the S-GW roaming user global charging profile.

```
[edit unified-edge gateways sgw MBG-SGW1 charging global-profile]
user@host# set roamer-profile MBG-SGW1-roaming
```

4. Configure the S-GW visiting user global charging profile.

```
[edit unified-edge gateways sgw MBG-SGW1 charging global-profile]
user@host# set visitor-profile MBG-SGW1-visiting
```

5. Configure the S-GW global charging profile selection order.

```
[edit unified-edge gateways sgw MBG-SGW1 charging global-profile]
user@host# set profile-selection-order static serving pgw-cg-addr
```

## Related Documentation

- [Configuring Offline Charging on page 443](#)
- [Configuring S-GW-Specific Charging Parameters on page 444](#)
- [Configuring S-GW Charging Traceoptions on page 448](#)
- [Configuring S-GW Local Persistent Storage Traceoptions on page 451](#)
- [Configuring GTP Prime for Transferring CDRs on page 453](#)
- [Configuring Persistent Storage on page 455](#)
- [Configuring Transport Profiles for Offline Charging on page 459](#)
- [Configuring Charging Trigger Events for Offline Charging on page 462](#)
- [Configuring CDR Attributes on page 464](#)
- [Configuring Charging Profiles on page 467](#)
- [Configuring Charging Profiles for APNs on page 469](#)
- [Tracing Charging Operations on page 470](#)
- [Charging Data Records on page 434](#)

## Configuring S-GW Charging Traceoptions

Charging tracing operations record detailed messages about the operation of Serving Gateway (S-GW) charging services on the MobileNext Broadband Gateway. You can trace various types of S-GW charging operations such as triggers, resources, configuration events, and other information. You can specify which trace operations are logged by including specific tracing flags and levels.

[Table 47 on page 448](#) describes the flags relating to the S-GW that you can include at the `[edit unified-edge gateways sgw gateway-name charging traceoptions flag]` hierarchy level.

**Table 47: S-GW Charging Trace Flags**

| Flag                      | Description                                  |
|---------------------------|----------------------------------------------|
| <code>all</code>          | Trace everything.                            |
| <code>cdr-encoding</code> | Trace Charging Detail Record (CDR) encoding. |
| <code>client-fsm</code>   | Trace client finite state machine (FSM).     |
| <code>config</code>       | Trace configuration events.                  |
| <code>fsm</code>          | Trace FSM events.                            |
| <code>general</code>      | Trace general events.                        |
| <code>group-fsm</code>    | Trace group FSM events.                      |
| <code>init</code>         | Trace initialization events.                 |

Table 47: S-GW Charging Trace Flags (*continued*)

|                        |                               |
|------------------------|-------------------------------|
| <b>ipc</b>             | Trace IPC events.             |
| <b>path-management</b> | Trace path management module. |
| <b>request</b>         | Trace requests.               |
| <b>resource</b>        | Trace resources.              |
| <b>response</b>        | Trace response.               |
| <b>timers</b>          | Trace timers.                 |
| <b>transport</b>       | Trace transport group.        |
| <b>triggers</b>        | Trace trigger information.    |

[Table 48 on page 449](#) describes the levels you can include.

Table 48: S-GW Charging Trace Levels

| Level          | Description                                        |
|----------------|----------------------------------------------------|
| <b>all</b>     | Match all levels.                                  |
| <b>error</b>   | Match error conditions.                            |
| <b>info</b>    | Match informational messages.                      |
| <b>notice</b>  | Match conditions that should be specially handled. |
| <b>verbose</b> | Match verbose messages.                            |
| <b>warning</b> | Match warning messages.                            |

To configure tracing options for charging operations:

1. Specify that you want to configure tracing options for charging operations.

```
[edit unified-edge gateways sgw MBG2 charging]
user@host# edit traceoptions
```



**NOTE:** You can use the `no-remote-trace` statement at this level to disable remote tracing capabilities.

2. Configure the filename for the trace file.

```
[edit unified-edge gateways sgw MBG2 charging traceoptions]
user@host# set file datapath-log
```

3. (Optional) Configure the maximum size of each trace file.

```
[edit unified-edge gateways sgw MBG2 charging traceoptions]
user@host# set file size 100m
```

---



**NOTE:** When a trace file (for example, `sgw-charging-log`) reaches its maximum size, it is renamed `sgw-charging-log.0`, then `sgw-charging-log.1`, and so on, until the maximum number of trace files is reached. The oldest archived file is then overwritten.

---

4. Configure the tracing flag.

```
[edit unified-edge gateways sgw MBG2 charging traceoptions]
user@host# set flag all
```

---



**NOTE:** You should use care when tracing all operations on a gateway. This can have a performance impact.

---

5. Configure the tracing level.

```
[edit unified-edge gateways sgw MBG2 charging traceoptions]
user@host# set level error
```

6. View the trace file.

```
user@host# file show /var/log/sgw-charging-log
```

#### Related Documentation

- [Configuring Offline Charging on page 443](#)
- [Configuring S-GW-Specific Charging Parameters on page 444](#)
- [Configuring S-GW Global Charging Profiles and Selection Order on page 446](#)
- [Configuring S-GW Local Persistent Storage Traceoptions on page 451](#)
- [Configuring GTP Prime for Transferring CDRs on page 453](#)
- [Configuring Persistent Storage on page 455](#)
- [Configuring Transport Profiles for Offline Charging on page 459](#)
- [Configuring Charging Trigger Events for Offline Charging on page 462](#)
- [Configuring CDR Attributes on page 464](#)
- [Configuring Charging Profiles on page 467](#)
- [Configuring Charging Profiles for APNs on page 469](#)
- [Tracing Charging Operations on page 470](#)
- [Charging Data Records on page 434](#)
- [Configuring S-GW Traceoptions on page 59](#)
- [Configuring S-GW Software Data Path Traceoptions on page 62](#)
- [Configuring S-GW GTP Traceoptions on page 338](#)
- [Configuring S-GW Local Persistent Storage Traceoptions on page 451](#)



## Configuring S-GW Local Persistent Storage Traceoptions

Local persistent storage tracing operations record detailed messages about the operation of Serving Gateway (S-GW) charging information storage services on the MobileNext Broadband Gateway. You can trace various types of S-GW local persistent storage operations such as file operations, journaling, mirroring, and other information. You can specify which trace operations are logged by including specific tracing flags and levels.

[Table 49 on page 451](#) describes the flags relating to the S-GW that you can include at the `[edit unified-edge gateways sgw gateway-name charging local-persistent-storage traceoptions flag]` hierarchy level.

**Table 49: S-GW Local Persistent Storage Trace Flags**

| Flag                   | Description                                   |
|------------------------|-----------------------------------------------|
| <b>all</b>             | Trace everything.                             |
| <b>connection</b>      | Trace connection establishment with peers.    |
| <b>file-operations</b> | Trace file open, write, and close operations. |
| <b>general</b>         | Trace miscellaneous operations.               |
| <b>journaling</b>      | Trace file journaling operations.             |
| <b>mirror</b>          | Trace mirroring operations.                   |

[Table 50 on page 451](#) describes the levels you can include.

**Table 50: S-GW Local Persistent Storage Trace Levels**

| Level          | Description                                        |
|----------------|----------------------------------------------------|
| <b>all</b>     | Match all levels.                                  |
| <b>error</b>   | Match error conditions.                            |
| <b>info</b>    | Match informational messages.                      |
| <b>notice</b>  | Match conditions that should be specially handled. |
| <b>verbose</b> | Match verbose messages.                            |
| <b>warning</b> | Match warning messages.                            |

To configure tracing options for local persistent storage operations:

1. Specify that you want to configure tracing options for local persistent storage operations.

`[edit unified-edge gateways sgw MBG2 charging local-persistent-storage]`

```
user@host# edit traceoptions
```



**NOTE:** You can use the `no-remote-trace` statement at this level to disable remote tracing capabilities.

2. Configure the filename for the trace file.

```
[edit unified-edge gateways sgw MBG2 charging local-persistent-storage traceoptions]  
user@host# set file datapath-log
```

3. (Optional) Configure the maximum size of each trace file.

```
[edit unified-edge gateways sgw MBG2 charging local-persistent-storage traceoptions]  
user@host# set file size 100m
```



**NOTE:** When a trace file (for example, `sgw-lps-log`) reaches its maximum size, it is renamed `sgw-lps-log.0`, then `sgw-lps-log.1`, and so on, until the maximum number of trace files is reached. The oldest archived file is then overwritten.

4. Configure the tracing flag.

```
[edit unified-edge gateways sgw MBG2 charging local-persistent-storage traceoptions]  
user@host# set flag all
```



**NOTE:** You should use care when tracing all operations on a gateway. This can have a performance impact.

5. Configure the tracing level.

```
[edit unified-edge gateways sgw MBG2 charging local-persistent-storage traceoptions]  
user@host# set level error
```

6. View the trace file.

```
user@host# file show /var/log/sgw-lps-log
```

#### Related Documentation

- [Configuring Offline Charging on page 443](#)
- [Configuring S-GW-Specific Charging Parameters on page 444](#)
- [Configuring S-GW Global Charging Profiles and Selection Order on page 446](#)
- [Configuring S-GW Charging Traceoptions on page 448](#)
- [Configuring GTP Prime for Transferring CDRs on page 453](#)
- [Configuring Persistent Storage on page 455](#)
- [Configuring Transport Profiles for Offline Charging on page 459](#)
- [Configuring Charging Trigger Events for Offline Charging on page 462](#)
- [Configuring CDR Attributes on page 464](#)

- [Configuring Charging Profiles on page 467](#)
- [Configuring Charging Profiles for APNs on page 469](#)
- [Tracing Charging Operations on page 470](#)
- [Charging Data Records on page 434](#)
- [Configuring S-GW Traceoptions on page 59](#)
- [Configuring S-GW Software Data Path Traceoptions on page 62](#)
- [Configuring S-GW GTP Traceoptions on page 338](#)
- [Configuring S-GW Charging Traceoptions on page 448](#)

## Configuring GTP Prime for Charging

To configure GPRS tunneling protocol (GTP) Prime to transfer Charging Data Records (CDRs), perform these tasks:

- [Configuring GTP Prime for Transferring CDRs on page 453](#)
- [Configuring GTP Prime Peers on page 454](#)

### Configuring GTP Prime for Transferring CDRs

CDRs are transferred to a charging gateway using GTP Prime or logged to a Routing Engine hard disk and eventually retrieved by a charging gateway using FTP.

To configure global GTP Prime options to transfer CDRs:

1. Specify that you want to configure GTP Prime properties for the gateway called MBG1.

```
[edit]
user@host# edit unified-edge gateways ggsn-pgw MBG1 charging gtp
```

2. Specify the destination port number of the charging gateway function (CGF) server.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging gtp]
user@host# set destination-port port-number
```

3. Specify the source interface from which GTP Prime packets will be sent.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging gtp]
user@host# set source-interface interface-name <ipv4-address>
```

4. Specify the transport protocol.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging gtp]
user@host# set transport-protocol (udp | tcp)
```

5. Specify the GTP Prime version.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging gtp]
user@host# set version (v0 | v1 | v2)
```

6. Specify the GTP Prime header type.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging gtp]
user@host# set header-type (long | short)
```

7. Specify that path management is disabled. This option cannot be used with the echo request interval.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging gtp]  
user@host# set no-path-management
```

8. Specify the GTP Prime echo request interval for path management.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging gtp]  
user@host# set echo-interval seconds
```

9. Specify the number of retries of GTP Prime messages upon timeout.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging gtp]  
user@host# set n3-requests requests
```

10. Specify the response timeout value for the GTP Prime request message.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging gtp]  
user@host# set t3-response response-interval
```

11. Specify the time to wait before declaring a CGF as down.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging gtp]  
user@host# set down-detect-time seconds
```

12. Specify the time after which to retry the connection to the CGF server.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging gtp]  
user@host# set reconnect-time seconds
```

13. Specify the maximum number of Data Record Transfer (DRT) messages awaiting an acknowledgment.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging gtp]  
user@host# set pending-queue-size queue-size
```

## Configuring GTP Prime Peers

CDRs are transferred to a charging gateway using GTP Prime. The charging gateway is the GTP Prime peer. The charging gateway peer inherits the global GTP Prime values. You configure the GTP Prime peer only if you want to override any of the global GTP Prime values.

To configure the GTP Prime peer to transfer CDRs:

1. Specify the name of the CGF peer for which you are configuring GTP Prime properties. Use this peer name to configure the peer order in the transport profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging gtp]  
user@host# edit peer peer-name
```

2. Specify the destination IPv4 address of the CGF peer.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging gtp peer peer-name]  
user@host# set destination-ipv4-address ip-address
```

3. (Optional) Specify any of the global GTP Prime options that you want to override for this charging gateway.

- Related Documentation**
- [Configuring Offline Charging on page 443](#)
  - [Configuring Transport Profiles for Offline Charging on page 459](#)
  - [Offline Charging Overview on page 431](#)

## Configuring Persistent Storage

You can store Charging Data Records (CDRs) locally on the Routing Engine hard disk. You must configure the persistent storage order in the transport profile before CDRs can be stored locally on the Routing Engine.

To configure local persistent storage for the CDRs, perform these tasks:

- [Configuring Local Persistent Storage on page 455](#)
- [Tracing Persistent Storage Operations on page 456](#)

### Configuring Local Persistent Storage

To configure local persistent storage of the file containing the CDRs:

1. Specify that you want to configure local persistent storage.

```
[edit]
user@host# edit unified-edge gateways ggsn-pgw MBG1 charging
local-persistent-storage-options
```

2. Specify the file age, in minutes.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging local-persistent-storage-options]
user@host# set file-age value
```

3. Specify the file size, in MB.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging local-persistent-storage-options]
user@host# set file-size value
```

4. Specify the number of CDRs for each file.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging local-persistent-storage-options]
user@host# set cdrs-per-file value
```

5. Specify that CDR log files are not replicated to the standby Routing Engine.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging local-persistent-storage-options]
user@host# set disable-replication
```

6. Specify the user authorized to access the files.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging local-persistent-storage-options]
user@host# set user-name username
```

7. Specify that CDR log files can be accessed for reading by all users.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging local-persistent-storage-options]
user@host# set world-readable
```

8. Specify the private extension for the filename.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging local-persistent-storage-options]
```

```
user@host# set file-name-private-extension string
```

- Specify whether the CDR file is shared across all nodes for a charging group or is unique to a charging group in each node.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging local-persistent-storage-options]
user@host# set file-creation-policy (unique-file | shared-file)
```

- Configure the CDR file format as 3GPP 32 297 format or raw ASN.1 format.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging local-persistent-storage-options]
user@host# set file-format (3gpp | raw-asn)
```

- Configure the disk policy for when the disk runs out of space. Specify the percentage and notification for the watermark levels. Notification can be to generate an SNMP alarm, a syslog, or both.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging local-persistent-storage-options]
user@host# set disk-space-policy watermark-level-1 (percentage) (syslog | snmp |
alarm)
user@host# set disk-space-policy watermark-level-2 (percentage) (syslog | snmp |
alarm)
user@host# set disk-space-policy watermark-level-3 (percentage) (syslog | snmp |
alarm)
```

## Tracing Persistent Storage Operations

To configure tracing operations for local persistent storage:

- Specify that you want to configure tracing options for charging operations.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging local-persistent-storage-options]
user@host# edit traceoptions
```

- (Optional) Configure the name for the file used for the trace output.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging local-persistent-storage-options
traceoptions]
user@host# set file filename
```

- (Optional) Configure flags to filter the operations to be logged.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging local-persistent-storage-options
traceoptions]
user@host# set flag flag
```

By default, only important events are logged. You can specify which trace operations are logged by including specific tracing flags. The following table describes the flags that you can include.

| Flag                   | Description                                                                                        |
|------------------------|----------------------------------------------------------------------------------------------------|
| <b>all</b>             | Trace all operations                                                                               |
| <b>connection</b>      | Trace connection establishment between the Routing Engine and all session DPCs for CDR file backup |
| <b>file-operations</b> | Trace file operations (open, write, close)                                                         |

| Flag              | Description                      |
|-------------------|----------------------------------|
| <b>general</b>    | Trace miscellaneous operations   |
| <b>journaling</b> | Trace file journaling operations |
| <b>mirror</b>     | Trace mirroring operations       |

4. (Optional) Configure the level of tracing.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging local-persistent-storage-options
traceoptions]
user@host# set level (all | critical | error | info | notice | verbose | warning)
```

#### Related Documentation

- [Configuring the Solid State Disk for Persistent Storage on page 457](#)
- [Configuring Offline Charging on page 443](#)
- [Configuring Transport Profiles for Offline Charging on page 459](#)
- [Offline Charging Overview on page 431](#)
- [Configuring S-GW-Specific Charging Parameters on page 444](#)
- [Configuring S-GW Global Charging Profiles and Selection Order on page 446](#)
- [Configuring S-GW Charging Traceoptions on page 448](#)
- [Configuring S-GW Charging Traceoptions on page 448](#)

## Configuring the Solid State Disk for Persistent Storage

You can use the Solid State Disk (SSD) on the Routing Engine for local persistent storage. You must configure the SSD (part number SSD-CDR-S) before Charging Data Records (CDRs) can be stored locally on the Routing Engine.



**NOTE:** If you do not want to format the existing content on the SSD, you must specify the **no-format** option when preparing the SSD.

To use the SSD for local persistent storage of CDRs, perform these tasks:

- [Initializing the Solid State Disk for Persistent Storage on page 457](#)
- [Ejecting the Solid State Disk on page 458](#)
- [Installing the Solid State Disk on page 458](#)

### Initializing the Solid State Disk for Persistent Storage

If the SSD on the Routing Engine is not plugged in before you start storing CDRs locally on the Routing Engine, you must initialize the SSD.

To initialize the SSD for local persistent storage when it has not been installed in the Routing Engine:

1. Power down the Routing Engine by pressing the Online/Offline button or entering the **shutdown -h now** command.
2. Install the SSD. For information about installing the SSD, see “Replacing an SSD Drive on an RE-A-1800 or RE-S-1800” in the Hardware Guide for your MX Series router.
3. Boot the Routing Engine.
4. Prepare the SSD to store CDRs.

```
user@host> request system storage unified-edge media prepare
```

---



**NOTE:** If you do not want to format the existing content on the SSD, you must specify the **no-format** option.

---

5. Enable the SSD to start storing CDRs.

```
user@host> request system storage unified-edge charging media start
```

## Ejecting the Solid State Disk

To eject the SSD from the Routing Engine:

1. Disable the SSD to close all open files and stop storing CDRs.

```
user@host> request system storage unified-edge charging media stop
```

2. Prepare the SSD for removal from the Routing Engine.

```
user@host> request system storage unified-edge media eject
```

3. Remove the SSD from the Routing Engine. For information about removing the SSD, see “Replacing an SSD Drive on an RE-A-1800 or RE-S-1800” in the Hardware Guide for your MX Series router.

## Installing the Solid State Disk

If the SSD on the Routing Engine is reinstalled on the Routing Engine after it was initialized, you must prepare the SSD to store CDRs.

To prepare the SSD for local persistent storage when it has been reinstalled on the Routing Engine:

1. Install the SSD. For information about installing the SSD, see “Replacing an SSD Drive on an RE-A-1800 or RE-S-1800” in the Hardware Guide for your MX Series router.
2. Prepare the SSD to store CDRs.

```
user@host> request system storage unified-edge media prepare
```

---



**NOTE:** If you do not want to format the existing content on the SSD, you must specify the **no-format** option.

---



3. Enable the SSD to start storing CDRs.

```
user@host> request system storage unified-edge charging media start
```

4. Reboot the Routing Engine.

#### Related Documentation

- [Configuring Persistent Storage on page 455](#)
- *request system storage unified-edge charging media start*
- *request system storage unified-edge charging media stop*
- *request system storage unified-edge media eject*
- *request system storage unified-edge media prepare*

## Configuring Transport Profiles for Offline Charging

A transport profile provides information for transporting offline Charging Data Records (CDRs) and online messages. Offline CDRs are transported from the charging data function (CDF) to the charging gateways or to local persistent storage, and online messages are transported between the Gateway GPRS Support Node (GGSN) Packet Data Network Gateway (P-GW) and the Online Charging System (OCS). A transport profile can be associated with one or more charging profiles. You can configure a maximum of eight transport profiles.



**NOTE:** The following configuration steps are applicable at both the [edit unified-edge gateways ggsn-pgw *gateway-name* charging] and the [edit unified-edge gateways sgw *gateway-name* charging] hierarchy levels. However, for clarity, they are presented only at the [edit unified-edge gateways ggsn-pgw *gateway-name* charging] hierarchy level. Unless explicitly stated otherwise, the configuration steps can be used with exactly the same syntax under both hierarchy levels.

To configure transport profiles for offline charging:

1. Specify the name of the transport profile that you are configuring for the gateway called MBG1.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging]
user@host# edit transport-profiles profile-name
```

The transport profile name can contain letters, numbers, and hyphens (-) and can be up to 128 characters long.

2. Specify a description for the transport profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles profile-name]
user@host# set description string
```

3. Specify that you want to configure offline charging in the transport profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles profile-name]
user@host# edit offline
```

4. Configure the charging function name for offline charging, which is used to select the transport profile for offline charging.

If either the primary or secondary charging functions obtained from the policy and charging rules function (PCRF) match the one configured here, then the transport profile is selected. If the names provided by the PCRF do not match, then the transport profile is not selected and the default transport profile is used.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
 transport-profile1 offline]
user@host# set charging-function-name function-name
```

5. Configure the transport parameters for offline CDRs.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
 transport-profile1 offline]
user@host# edit charging-gateways
```

- a. Configure the order in which the charging gateways are selected. The charging gateway must be defined as a GTP Prime peer. The highest-priority peer is selected first as the active charging gateway. When the active charging gateway goes down, the next higher-priority peer is selected. If all the charging gateways are down and you have configured local persistent storage, then the CDRs are stored on the Routing Engine.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
 transport-profile1 offline charging-gateways]
user@host# set peer-order peer charging-gateway-peer-name
```

- b. Specify the time that the CDF must wait before switching back to a higher-priority peer from a lower-priority peer that has become the active charging gateway.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
 transport-profile1 offline charging-gateways]
user@host# set switch-back-time seconds
```

The range for the time that the CDF must wait before switching to a higher-priority peer is 0 through 300 seconds.

- c. Specify that the persistent storage order is local (on the Routing Engine). You must configure the persistent storage order before CDRs can be stored locally on the Routing Engine.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
 transport-profile1 offline charging-gateways]
user@host# set persistent-storage-order local-storage
```

- d. Configure the CDR format version. The charging format implemented in the 3GPP Release 8 specifications (r8) is the default format version.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
 transport-profile1 offline charging-gateways]
user@host# set cdr-release (r7 | r8 | r9 | r99)
```



**NOTE:** 3GPP release versions 7, 9, and 99 are only applicable to the GGSN and P-GW (not to the S-GW), while 3GPP release version 8 is applicable to the GGSN, P-GW, and S-GW.

---

- e. Specify the maximum number of CDRs that can be added to a Data Record Transfer (DRT) message before it is transmitted. A DRT message containing the CDRs is transmitted from the CDF to the charging gateway function (CGF) server, when the **cdr-aggregation-limit** or the **mtu** size is reached (whichever comes first).

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
 transport-profile1 offline charging-gateways]
user@host# set cdr-aggregation-limit value
```

The range for the CDR aggregation limit is 1 through 16.

- f. Configure the maximum transmission unit (MTU), in bytes, of the DRT message.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
 transport-profile1 offline charging-gateways]
user@host# set mtu value
```

The range for the MTU is 300 through 8000 bytes.

6. Specify the maximum number of containers to limit for each CDR.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
 transport-profile1 offline]
user@host# set container-limit value
```

The range for the maximum number of containers for a CDR is 1 through 15.

7. Specify the number of SGSN or S-GW changes that can occur before the CDR is updated and closed.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
 transport-profile1 offline]
user@host# set sgsn-sgw-change-limit value
```

The range for the maximum number of SGSN or S-GW changes that can occur is 1 through 5.



**NOTE:** This statement is not applicable to the Serving Gateway (S-GW).

#### Related Documentation

- [Charging Profiles on page 438](#)
- [Configuring Charging Profiles on page 467](#)
- [Configuring GTP Prime for Charging on page 453](#)
- [Configuring Offline Charging on page 443](#)
- [Configuring Persistent Storage on page 455](#)
- [Configuring S-GW-Specific Charging Parameters on page 444](#)
- [Configuring S-GW Global Charging Profiles and Selection Order on page 446](#)
- [Configuring S-GW Charging Traceoptions on page 448](#)
- *offline (Transport Profiles)*
- *transport-profiles*

## Configuring Charging Trigger Events for Offline Charging

---

A trigger profile defines the charging events that cause offline Charging Data Record (CDR) changes and attributes for online charging. For offline CDRs, a trigger profile determines the events that trigger the creation of a Charging Data Record (CDR), the addition of a container to a CDR, and the closure of a CDR. You can configure up to a maximum of 16 trigger profiles.



**NOTE:** The following configuration steps are applicable at both the [edit unified-edge gateways ggsn-pgw *gateway-name* charging] and the [edit unified-edge gateways sgw *gateway-name* charging] hierarchy levels. However, for clarity, they are presented only at the [edit unified-edge gateways ggsn-pgw *gateway-name* charging] hierarchy level. Unless explicitly stated otherwise, the configuration steps can be used with exactly the same syntax under both hierarchy levels.

To configure trigger profiles for offline charging:

1. Specify the name of the trigger profile that you are configuring for the gateway called MBG1.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging]
user@host# edit trigger-profiles profile-name
```

The trigger profile name can contain letters, numbers, and hyphens (-) and can be up to 128 characters long.

2. Specify a description for the trigger profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name]
user@host# set description string
```

3. Configure the default charging method to be used for subscribers attached to the trigger profile. The broadband gateway uses the configured default charging method only when the policy and charging rules function (PCRF) or the static policy and charging enforcement function (PCEF) policy do not provide a charging method.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name]
user@host# set charging-method (both | none | offline | online)
```

If you do not configure this statement, then offline charging is enabled by default.

4. Configure offline charging in the trigger profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name]
user@host# edit offline
```

5. Specify a time limit for closing the CDR. A value of zero (0) disables this trigger.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
offline]
user@host# set time-limit seconds
```

The range for the activation of the time limit is 600 through 65,535 seconds.

6. Specify the PDP context or bearer information changes that do not trigger charging data updates. All of these changes trigger a container or CDR closure by default.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
  offline]
user@host# set exclude [bearer-information-change]
```

You can specify more than one trigger to exclude in a single line. For example, to exclude the PLMN change and QoS change (in a trigger profile called *trigger-profile-1*) from the CCR messages:

```
[edit unified-edge gateways ggsn-pgw MBG-PGW1 charging trigger-profiles
  trigger-profile-1 offline]
user@host# set exclude plmn-change qos-change
```

[Table 51 on page 463](#) describes the bearer information changes that can be ignored for charging data updates.

**Table 51: Bearer Information Changes**

| Bearer Information Change   | Description                                                                                                                                                                          |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>dcca-events</b>          | Diameter Credit Control Application (DCCA) events<br><br><b>NOTE:</b> This trigger is applicable only to the Gateway GPRS Support Node (GGSN) or Packet Data Network Gateway (P-GW). |
| <b>ms-timezone-change</b>   | Mobile Station (MS) time zone change                                                                                                                                                 |
| <b>plmn-change</b>          | Public land mobile network (PLMN) change                                                                                                                                             |
| <b>qos-change</b>           | Quality-of-service (QoS) change                                                                                                                                                      |
| <b>rat-change</b>           | Radio Access Technology (RAT) change                                                                                                                                                 |
| <b>sgsn-mme-change</b>      | Serving GPRS Support Node (SGSN) or Mobility Management Entity (MME) change<br><br><b>NOTE:</b> This trigger is applicable only to the S-GW.                                         |
| <b>sgsn-sgw-change</b>      | SGSN or S-GW limit change<br><br><b>NOTE:</b> This trigger is applicable only to the GGSN or P-GW.                                                                                   |
| <b>user-location-change</b> | User location information change                                                                                                                                                     |

7. Specify a volume limit trigger for bandwidth, in bytes.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
  offline]
user@host# set volume-limit value
```

The range for the volume limit is 1 through 4,294,967,295 bytes.

8. Specify the direction for the volume limit trigger. If you specify **both**, the volume limit applies to the combined amount of uplink and downlink traffic.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
offline]
user@host# set volume-limit direction (both | uplink)
```

9. Configure the list of times to update CDRs when the tariffs change within a day. These times can be specified in a minimum of 15-minute increments. Specify the tariff time changes in the format *hh:mm*, where *hh* is 00 through 23 (00 is midnight) and *mm* is 00 through 59. The specified time is local time. You can configure up to a maximum of 24 tariff time changes.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name]
user@host# set tariff-time-list hh:mm
```

For example:

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
tariff-time-list]
user@host# set tariff-time-list 21:00
user@host# set tariff-time-list 07:00
```

**Related  
Documentation**

- [Charging Profiles on page 438](#)
- [Configuring Charging Profiles on page 467](#)
- [Configuring Offline Charging on page 443](#)
- [Configuring S-GW-Specific Charging Parameters on page 444](#)
- [Configuring S-GW Global Charging Profiles and Selection Order on page 446](#)
- [Configuring S-GW Charging Traceoptions on page 448](#)
- *offline (Trigger Profiles)*
- *trigger-profiles (GGSN or P-GW)*
- *trigger-profiles (Serving Gateway)*

---

## Configuring CDR Attributes

A Charging Data Record (CDR) profile defines the attributes in each CDR.

To configure CDR profiles:



**NOTE:** The following configuration steps are applicable at both the [edit unified-edge gateways ggsn-pgw *gateway-name* charging] and the [edit unified-edge gateways sgw *gateway-name* charging] hierarchy levels. However, for clarity, they are presented only at the [edit unified-edge gateways ggsn-pgw *gateway-name* charging] hierarchy level. Unless explicitly stated otherwise, the configuration steps can be used with exactly the same syntax under both hierarchy levels.

1. Specify the name of the CDR profile that you are configuring for the gateway called MBG1.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging]
user@host# edit cdr-profiles profile-name
```

The CDR profile name can contain letters, numbers, and hyphens (-) and can be up to 128 characters long.

2. Specify a description for the profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging cdr-profiles profile-name]
user@host# set description string
```

3. Enable reduced partial CDR (RPC) generation.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging cdr-profiles profile-name]
user@host# set enable-reduced-partial-cdrs
```

4. Set optional attributes to exclude from the CDR. You can specify the excluded attributes so that you can manage the size of the CDR. By default, all attributes are included in the CDR.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging cdr-profiles profile-name]
user@host# set exclude-attributes [attribute]
```

[Table 52 on page 465](#) describes the attributes that can be excluded from CDRs.

**Table 52: Attribute Exclusions**

| Attribute               | Information in CDRs                                   |
|-------------------------|-------------------------------------------------------|
| apn-ni                  | Access point name (APN) network identifier            |
| apn-selection-mode      | APN selection mode                                    |
| cc-selection-mode       | Charging characteristic selection mode                |
| dynamic-address         | Dynamic Packet Data Protocol (PDP) address indication |
| list-of-service-data    | List of service data                                  |
| list-of-traffic-volumes | List of traffic volumes                               |

Table 52: Attribute Exclusions (*continued*)

| Attribute                           | Information in CDRs                                                                 |
|-------------------------------------|-------------------------------------------------------------------------------------|
| <b>lrsn</b>                         | Local record sequence number                                                        |
| <b>ms-time-zone</b>                 | Mobile station (MS) time zone                                                       |
| <b>network-initiation</b>           | Network initiation flag                                                             |
| <b>node-id</b>                      | Node identifier                                                                     |
| <b>pdn-connection-id</b>            | Packet data network (PDN) connection ID                                             |
| <b>pdppdn-type</b>                  | PDP or PDN type                                                                     |
| <b>pgw-plmn-identifier</b>          | P-GW public land mobile network (PLMN) identifier field                             |
| <b>ps-furnish-info</b>              | PS Furnish Info (where PS stands for packet switched)                               |
| <b>rat-type</b>                     | Radio Access Technology (RAT) type                                                  |
| <b>record-sequence-number</b>       | Record sequence number                                                              |
| <b>served-imeisv</b>                | Served International Mobile Equipment Identity and Software Version Number (IMEISV) |
| <b>served-msisdn</b>                | Served mobile station ISDN (MSISDN)                                                 |
| <b>served-pdppdn-address</b>        | Served PDP context or IP-CAN bearer address                                         |
| <b>served-pdp-address-extension</b> | Served PDP context or IP-CAN bearer address extension                               |
| <b>serving-node-plmn-identifier</b> | Serving node PLMN identifier field                                                  |
| <b>start-time</b>                   | Time when session established; added to first CDR                                   |
| <b>stop-time</b>                    | Time when session terminated; added to last CDR                                     |
| <b>user-location-information</b>    | User location information                                                           |

- Specify the format of the node identifier (ID) in the CDR. The node identifier indicates the node that generated the CDR.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging cdr-profiles profile-name]
user@host# set node-id hostname
```



**NOTE:**

- The node identifier can be configured as one of the following:
  - hostname—Hostname of the node that generated the CDR.
  - hostname-spic—Hostname of the node that generated the CDR and the ID of the services PIC on which the CDR was triggered, delimited by a colon (:).
  - ipaddress-spic—IP address of the node that generated the CDR and the ID of the services PIC on which the CDR was triggered, delimited by a colon (:).
- If you do not include the `node-id` statement, then the IP address of the node generating the CDR and the ID of the services PIC on which the CDR was triggered, with a colon (:) as a delimiter, are used as the node identifier.

6. Specify that the broadband gateway includes the requested access point name (APN) in the CDRs of subscribers attached to the CDR profile. Therefore, when the APN type is virtual, the broadband gateway includes the requested or virtual APN in the CDRs.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging cdr-profiles profile-name]
user@host# set report-requested-apn
```



**NOTE:** If you do not include the `report-requested-apn` statement, then, by default, the broadband gateway includes only the real APN in the CDR. (For virtual APNs, the real APN to which the virtual APN is mapped is included in the CDR.)

**Related  
Documentation**

- *cdr-profiles*
- [Configuring Charging Profiles on page 467](#)
- [Configuring Offline Charging on page 443](#)
- [Charging Profiles on page 438](#)
- [Configuring S-GW-Specific Charging Parameters on page 444](#)
- [Configuring S-GW Global Charging Profiles and Selection Order on page 446](#)
- [Configuring S-GW Charging Traceoptions on page 448](#)
- [Tracing Charging Operations on page 470](#)

## Configuring Charging Profiles

A charging profile defines the charging behavior applied to a mobile subscriber. The charging profile includes a transport profile, a Charging Data Record (CDR) profile, one or more trigger profiles, and other default service-aware charging information.



**NOTE:** The following configuration steps are applicable at both the [edit unified-edge gateways ggsn-pgw *gateway-name* charging] and the [edit unified-edge gateways sgw *gateway-name* charging] hierarchy levels. However, for clarity, they are presented only at the [edit unified-edge gateways ggsn-pgw *gateway-name* charging] hierarchy level. Unless explicitly stated otherwise, the configuration steps can be used with exactly the same syntax under both hierarchy levels.

To configure charging profiles:

1. Specify the name of the charging profile that you are configuring for the gateway called MBG1.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging]
user@host# edit charging-profiles profile-name
```

The charging profile name can contain letters, numbers, and hyphens (-) and can be up to 128 characters long.

2. Specify a profile identifier that is matched against the GPRS tunneling protocol (GTP) charging characteristic or authentication, authorization, and accounting (AAA) charging profile number. The profile identifier must be specified and it must be a unique value across all charging profiles defined for a gateway.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging charging-profiles profile-name]
user@host# set profile-id profile-id
```

3. Specify the transport profile referenced by this charging profile. The transport profile must be specified and must be previously configured on the broadband gateway.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging charging-profiles profile-name]
user@host# set transport-profile profile-name
```

4. (Optional) Specify a description for the profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging charging-profiles profile-name]
user@host# set description string
```

5. (Optional) Specify the default rating group, which is used for charging service data containers. This configuration is not applicable for the S-GW.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging charging-profiles profile-name]
user@host# set default-rating-group integer
```

If no default rating group is specified, then **RG 0** is sent in the Credit Control Request (CCR) message.

6. (Optional) Specify the default service identifier for the service or the service component, which is used for charging service data containers. This configuration is not applicable for the S-GW.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging charging-profiles profile-name]
user@host# set default-service-id integer
```

If no default service identifier is specified, then **Service ID 0** is sent in the Credit Control Request (CCR) message.

7. (Optional) Specify the CDR profile referenced by this charging profile. The CDR profile must be previously configured on the gateway.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging charging-profiles profile-name]
user@host# set cdr-profile profile-name
```

8. (Optional) Specify one or more trigger profiles to be referenced by this charging profile. The trigger profiles must be previously configured on the gateway.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging charging-profiles profile-name]
user@host# set trigger-profile profile-name
```

9. (Optional) Specify one or more rating group identifiers that should be associated with a trigger profile. The rating group is used to select the trigger profile to be associated with a charging profile. If the rating group identifier received by the broadband gateway matches the rating group identifier configured here, then the trigger profile with which the rating group identifier is associated is linked to the charging profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging charging-profiles profile-name
trigger-profile profile-name]
user@host# set rating-group [value]
```

#### Related Documentation

- [Configuring Offline Charging on page 443](#)
- [Configuring S-GW-Specific Charging Parameters on page 444](#)
- [Configuring S-GW Global Charging Profiles and Selection Order on page 446](#)
- [Configuring S-GW Charging Traceoptions on page 448](#)
- [Configuring S-GW Charging Traceoptions on page 448](#)
- [charging-profiles](#)
- [Charging Profiles on page 438](#)

## Configuring Charging Profiles for APNs

You can configure charging profiles that apply to access point names (APNs) that are used for the default profile, home subscribers, roaming subscribers, and visiting subscribers.

To configure charging profiles for APNs:

1. Specify that you want to configure charging profiles for a particular APN.

```
[edit]
user@host# edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-name
charging
```

2. Specify the name of the default charging profile. The charging profile must be defined.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-name charging]
user@host# set default-profile profile-name
```

3. Specify the name of the charging profile for home subscribers roaming in other public land mobile networks (PLMNs). The charging profile must be defined.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-name charging]
user@host# set home-profile profile-name
```

4. Specify the name of the charging profile for roaming subscribers between PLMNs. The charging profile must be defined.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-name charging]
user@host# set roamer-profile profile-name
```

5. Specify the name of the charging profile for visiting subscribers from other PLMNs. The charging profile must be defined.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-name charging]
user@host# set visitor-profile profile-name
```

6. Specify the profile selection order. You can order the selections by the charging profile sent by the RADIUS server (radius), the charging profile sent by the SGSN or Serving Gateway (serving), or the locally configured charging profile (static).

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-name charging]
user@host# set profile-selection-order [(serving | radius | static)]
```

#### Related Documentation

- [Configuring Offline Charging on page 443](#)
- [Charging Profiles on page 438](#)
- [Configuring S-GW-Specific Charging Parameters on page 444](#)
- [Configuring S-GW Global Charging Profiles and Selection Order on page 446](#)
- [Configuring S-GW Charging Traceoptions on page 448](#)
- [Configuring S-GW Charging Traceoptions on page 448](#)

---

## Tracing Charging Operations

Charging tracing operations track mobile charging operations and record them in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

All log files are located in the `/var/log` directory. You cannot change the directory in which trace files are located. When the trace file reaches its maximum size, a `.0` is appended to the filename, then a new file is created with a `.1`, and finally a `.2`. When the maximum number of trace files is reached, the oldest trace file is overwritten.



**NOTE:** You should use care when tracing charging operations because it can have a performance impact.

---

To configure charging tracing operations:

1. Specify that you want to configure tracing options for charging operations.

```
[edit]
user@host# edit unified-edge gateways ggsn-pgw MBG1 charging traceoptions
```

2. (Optional) Configure the name for the file used for the trace output.
3. (Optional) Configure flags to filter the operations to be logged.

The mobile charging traceoptions configuration tasks are described in the following topics:

- [Configuring the Trace Log Filename on page 471](#)
- [Configuring the Tracing Flags on page 471](#)

## Configuring the Trace Log Filename

By default, the name of the file that records trace output for mobile charging is **mobile-smd**. You can specify a different name with the **file** option to distinguish trace output for different session Dense Port Concentrators (DPCs). For example, you can specify the filename in the format *filename-msnumberfpcnumberpicnumber*.

To configure the filename for mobile charging tracing operations:

- Specify the name of the file used for the trace output.  

```
[edit unified-edge gateways ggsn-pgw MBG1 charging traceoptions]
user@host# set file filename
```

## Configuring the Tracing Flags

To configure the flags for the events to be logged:

- Configure the flags.  

```
[edit unified-edge gateways ggsn-pgw MBG1 charging traceoptions]
user@host# set flag flag
```

By default, only important events are logged. You can specify which trace operations are logged by including specific tracing flags. [Table 53 on page 471](#) describes the flags that you can include.

**Table 53: Charging Tracing Flags**

| Flag                | Description                             |
|---------------------|-----------------------------------------|
| <b>all</b>          | Trace all operations                    |
| <b>cdr-encoding</b> | Trace CDR encoding                      |
| <b>client-fsm</b>   | Trace client finite state machine (FSM) |
| <b>config</b>       | Trace configuration events              |
| <b>fsm</b>          | Trace FSM                               |
| <b>general</b>      | Trace general flow                      |
| <b>group-fsm</b>    | Trace group FSM                         |

Table 53: Charging Tracing Flags (*continued*)

| Flag                   | Description                                     |
|------------------------|-------------------------------------------------|
| <b>init</b>            | Trace initialization events                     |
| <b>ipc</b>             | Trace IPC                                       |
| <b>online</b>          | Trace Gy active session management (ASM) module |
| <b>path-management</b> | Trace path management module                    |
| <b>resource</b>        | Trace resources                                 |
| <b>timers</b>          | Trace timers                                    |
| <b>tpm</b>             | Trace online processing module                  |
| <b>transport</b>       | Trace transport group                           |
| <b>triggers</b>        | Trace trigger information                       |

**Related  
Documentation**

- [Configuring Offline Charging on page 443](#)
- [Configuring S-GW-Specific Charging Parameters on page 444](#)
- [Configuring S-GW Global Charging Profiles and Selection Order on page 446](#)
- [Configuring S-GW Charging Traceoptions on page 448](#)
- [Configuring S-GW Charging Traceoptions on page 448](#)

## Configuring Online Charging

You can configure the charging function on the MobileNext Broadband Gateway. The broadband gateway supports the configuration of online charging, which enables real-time charging of subscribers. The online charging configuration determines how online messages are transported between the broadband gateway and the Online Charging System (OCS), what the gateway does during credit control failure, and other miscellaneous attributes. The Gy interface connects the Gateway GPRS Support Node (GGSN) or Packet Data Network Gateway (P-GW) and the OCS.

To configure the broadband gateway for online charging:

- Configure the transport profile, which specifies how online charging messages between the GGSN or P-GW and the OCS are transported.
- (Optional) Configure the trigger profile, which specifies the credit control failure handling parameters and other miscellaneous online charging attributes.

- Configure the charging profile, which specifies the charging behavior to apply based on profiles included in the charging profile. The included profiles must be previously configured on the broadband gateway.
- Configure tracing for charging operations.

**Related  
Documentation**

- [Configuring Charging Profiles on page 467](#)
- [Configuring Charging Trigger Events for Online Charging on page 476](#)
- [Configuring Transport Profiles for Online Charging on page 473](#)
- [Example: Configuring Online Charging on page 486](#)
- [Online Charging Overview on page 433](#)
- [Tracing Charging Operations on page 470](#)

## Configuring Transport Profiles for Online Charging

A transport profile provides information for transporting offline Charging Data Records (CDRs) and online messages. Offline CDRs are transported from the charging data function (CDF) to the charging gateways or to local persistent storage, and online messages are transported between the Gateway GPRS Support Node (GGSN) Packet Data Network Gateway (P-GW) and the Online Charging System (OCS). A transport profile can be associated with one or more charging profiles. You can configure a maximum of eight transport profiles.

To configure transport profiles for online charging:

1. Specify the name of the transport profile that you are configuring for the gateway called MBG1.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging]
user@host# edit transport-profiles profile-name
```

The transport profile name can contain letters, numbers, and hyphens (-) and can be up to 128 characters long.

2. Specify a description for the transport profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles profile-name]
user@host# set description string
```

3. Specify that you want to configure online charging in the transport profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles profile-name]
user@host# edit online
```

4. (Optional) Specify that the broadband gateway reports both active and inactive rating groups to the OCS on bearer termination.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
transport-profile1 online]
user@host# set all-rgs-on-termination
```

If you do not include the **all-rgs-on-termination** statement, then, by default, the broadband gateway reports only the active rating groups to the OCS on bearer termination.

5. (Optional) Configure the charging function names for online charging, which are used to select the transport profile for online charging.

If either the primary or secondary charging functions obtained from the policy and charging rules function (PCRF) match the one configured here, then the transport profile is selected. If the names provided by the PCRF do not match, then the transport profile is not selected and the default transport profile is used.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
transport-profile1 online]
user@host# set charging-function-name function-name
```

6. Associate a previously configured Diameter Gy profile with the transport profile. The Diameter Gy profile configuration associated with the transport profile determines the OCS with which the GGSN or P-GW interacts.

The Diameter Gy profile must be specified and must be previously configured at the **[edit unified-edge diameter-profiles gy-profile]** hierarchy level.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
transport-profile1 online]
user@host# set diameter-profile diameter-gy-profile-name
```

7. (Optional) Specify that no Multiple Services Credit Control (MSCC) attribute-value pairs (AVPs) are included in the Credit Control Request-Terminate (CCR-T) messages sent from the broadband gateway to the OCS.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
transport-profile1 online]
user@host# set no-mscc-in-ccrt
```

If you include the **no-mscc-in-ccrt** statement, the broadband gateway first sends the MSCC AVPs in the CCR-Update (CCR-U) message (to report usage), and then sends the CCR-T message to the OCS. If you do not include this statement, then the broadband gateway sends the MSCC AVPs in the CCR-T messages (to report usage).

8. (Optional) Specify that the broadband gateway requests quota (for a rating group) from the OCS only on receipt of the first packet matching that rating group.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
transport-profile1 online]
user@host# set quota-request-on-first-packet
```

If you do not include the **quota-request-on-first-packet** statement, then, by default, broadband gateway requests quota from the OCS when the rating group is created.

9. (Optional) Specify that the broadband gateway sends CCR-Initial (CCR-I) messages to the OCS only on receipt of the first packet for any rating group of the bearer.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
transport-profile1 online]
user@host# set send-ccri-on-first-packet
```



If you do not include the **send-ccri-on-first-packet** statement, then the broadband gateway sends the CCR-I messages to the OCS to authorize the bearer during bearer establishment. In addition, if the **quota-request-on-first-packet** statement is configured, the broadband gateway sends the CCR-I messages without any MSCC AVPs included.

10. (Optional) Configure the service context identifier (ID) attribute-value pair (AVP). The broadband gateway sends this AVP in all Credit Control Request (CCR) messages to the OCS.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
 transport-profile1 online]
user@host# set service-context-id service-context-id-avp
```

The service context ID can be a maximum of 100 characters. If you do not configure the service context ID, then the default service context ID (9.32251@3gpp.org) is sent in CCR messages.

11. (Optional) Configure whether online charging sessions should fail over to an alternate server or not, when failure occurs during an ongoing credit control session. The alternate server is selected based on the configuration in the Diameter profile that is associated with the transport profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
 transport-profile1 online]
user@host# set session-failover-not-supported
```

If you do not include the **session-failover-not-supported** statement, the failover of online charging sessions to an alternative server is enabled by default.

12. (Optional) Specify that only one MSCC AVP is included in the CCR messages sent from the broadband gateway to the OCS.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
 transport-profile1 online]
user@host# set single-mscc
```

If you do not include the **single-mscc** statement, then, by default, the broadband gateway includes one or more MSCC AVPs in CCR messages.

13. (Optional) Specify the time (in seconds) that the broadband gateway waits for a response from the OCS before timing out.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
 transport-profile1 online]
user@host# set tx-timeout timeout
```

The range for the time that the broadband gateway waits for a response is 0 through 300 seconds.

#### Related Documentation

- [Configuring Online Charging on page 472](#)
- [Example: Configuring Online Charging on page 486](#)
- [Online Charging Overview on page 433](#)
- *online (Transport Profiles)*
- *transport-profiles*

## Configuring Charging Trigger Events for Online Charging

---

A trigger profile defines the charging events that cause offline Charging Data Record (CDR) changes, and the attributes for online charging. You can configure up to a maximum of 16 trigger profiles.



**NOTE:** The configuration of the trigger profile for online charging is optional.

You must perform the following procedure before you can configure online charging trigger attributes.

To configure the trigger profile for online charging:

1. Specify the name of the trigger profile that you are configuring for the gateway called MBG1.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging]
user@host# edit trigger-profiles profile-name
```

The trigger profile name can contain letters, numbers, and hyphens (-) and can be up to 128 characters long.

2. (Optional) Specify a description for the trigger profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name]
user@host# set description string
```

3. (Optional) Configure the default charging method to be used for subscribers attached to the trigger profile. The broadband gateway uses the configured default charging method only when the policy and charging rules function (PCRF) or the static policy and charging enforcement function (PCEF) policy does not provide a charging method.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name]
user@host# set charging-method (both | none | offline | online)
```

If you do not configure this statement, then offline charging is enabled by default.

4. Configure online charging in the trigger profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name]
user@host# edit online
```

To configure trigger attributes for online charging, you configure the credit control failure handling parameters and miscellaneous attributes such as the measurement method, quota threshold, reporting level, and so on. This topic includes the following tasks:

- [Configuring Credit Control Failure Handling Parameters on page 476](#)
- [Configuring Miscellaneous Online Charging Trigger Events on page 480](#)

## Configuring Credit Control Failure Handling Parameters

Credit control failure handling parameters determine what the broadband gateway does during credit control failure. If the Online Charging System (OCS) responds with a result code that is not successful, then actions configured for specific result codes are performed.

If the OCS does not respond to Credit Control Request (CCR) messages, then other configured actions are performed.

To configure credit control failure handling parameters:

1. Specify that the broadband gateway blocks traffic for a rating group pending reauthorization when the quota is exhausted.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online cc-failure-handling]
user@host# set block-traffic-pending-reauth-no-quota
```

2. Configure the actions to be carried out by the broadband gateway when the initial Credit Control Request fails.



**NOTE:** You can configure only one of the following actions.

- a. Specify that offline charging is used to charge subscribers. In this case, online charging is disabled for the subscriber. Optionally, you can also specify that the subscriber session is extended until the grace quota elapses. After the grace quota elapses, the session is terminated and the subscriber is charged using offline charging.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online cc-failure-handling]
user@host# set initial-request convert-to-offline
user@host# set initial-request convert-to-offline grant-grace-quota
```

- b. Optionally, specify that online charging is disabled, and that offline charging, if enabled, is used to charge subscribers. If offline charging is not enabled, then no charging is applied to the subscriber.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online cc-failure-handling]
user@host# set initial-request disable-online-charging
```

- c. Optionally, specify that the subscriber session is extended until the grace quota elapses. After the grace quota elapses, the session is terminated and the subscriber is charged using offline charging.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online cc-failure-handling]
user@host# set initial-request grant-grace-quota
```

3. Specify that the broadband gateway overrides the credit control failure handling parameters received from the OCS and uses the parameters configured locally on the gateway.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online cc-failure-handling]
user@host# set override
```

4. Configure the actions to be performed based on the Diameter Result-Code attribute-value pair (AVP) received from the OCS:

- a. Specify that the rating group is blacklisted when the OCS sends a Diameter Authorization Rejected message to the gateway. Optionally, you can also specify that the gateway retries with the OCS after the configured time elapses.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online cc-failure-handling]
user@host# set result-code-based-action authorization-rejected blacklist
user@host# set result-code-based-action authorization-rejected blacklist
retry-timer
```

For example, to configure the gateway to blacklist the rating group and retry with the OCS after 300 seconds (5 minutes):

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online cc-failure-handling]
user@host# set result-code-based-action authorization-rejected blacklist 300
```

- b. Specify that, if the result code is Diameter Credit Control Not Applicable, the gateway disables online charging and enables offline charging. Optionally, you can also specify that the subscriber session is extended until the grace quota elapses. After the grace quota elapses, the session is terminated and the subscriber is charged using offline charging.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online cc-failure-handling]
user@host# set result-code-based-action credit-control-not-applicable
convert-to-offline
user@host# set result-code-based-action credit-control-not-applicable
convert-to-offline grant-grace-quota
```

- c. Specify that the rating group is blacklisted when the OCS sends a Diameter Credit Limit Reached message to the gateway. Optionally, you can also specify that the gateway retries with the OCS after the configured time elapses.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online cc-failure-handling]
user@host# set result-code-based-action credit-limit-reached blacklist
user@host# set result-code-based-action credit-limit-reached blacklist retry-timer
```

- d. Specify the actions to be carried by the gateway when the OCS sends a Diameter End User Service Denied message.



**NOTE:** You can configure only one of the following actions.

---

- a. Specify that offline charging is used to charge subscribers. In this case, online charging is disabled for the subscriber. Optionally, you can also specify that the subscriber session is extended until the grace quota elapses. After the grace quota elapses, the session is terminated and the subscriber is charged using offline charging.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online cc-failure-handling]
user@host# set end-user-service-denied convert-to-offline
user@host# set end-user-service-denied convert-to-offline grant-grace-quota
```

- b. Optionally, specify that online charging is disabled, and that offline charging, if enabled, is used to charge subscribers. If offline charging is not enabled, then no charging is applied to the subscriber.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online cc-failure-handling]
user@host# set end-user-service-denied disable-online-charging
```

- e. Specify the actions to be carried out by the gateway when the OCS sends a Diameter User Unknown message.



**NOTE:** You can configure only one of the following actions.

- a. Specify that offline charging is used to charge subscribers. In this case, online charging is disabled for the subscriber. Optionally, you can also specify that the subscriber session is extended until the grace quota elapses. After the grace quota elapses, the session is terminated and the subscriber is charged using offline charging.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online cc-failure-handling]
user@host# set user-unknown convert-to-offline
user@host# set user-unknown convert-to-offline grant-grace-quota
```

- b. Optionally, specify that online charging is disabled, and that offline charging, if enabled, is used to charge subscribers. If offline charging is not enabled, then no charging is applied to the subscriber.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online cc-failure-handling]
user@host# set user-unknown disable-online-charging
```

- 5. Configure the actions to be carried out by the broadband gateway when the Credit Control Request-Update fails.



**NOTE:** You can configure only one of the following actions.

- a. Specify that offline charging is used to charge subscribers. In this case, online charging is disabled for the subscriber. Optionally, you can also specify that the subscriber session is extended until the grace quota elapses. After the grace quota elapses, the session is terminated and the subscriber is charged using offline charging.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online cc-failure-handling]
user@host# set update-request convert-to-offline
user@host# set update-request convert-to-offline grant-grace-quota
```

- b. Optionally, specify that online charging is disabled, and that offline charging, if enabled, is used to charge subscribers. If offline charging is not enabled, then no charging is applied to the subscriber.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online cc-failure-handling]
```

```
user@host# set update-request disable-online-charging
```

- c. Optionally, specify that the subscriber session is extended until the grace quota elapses. After the grace quota elapses, the session is terminated and the subscriber is charged using offline charging.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online cc-failure-handling]
```

```
user@host# set update-request grant-grace-quota
```

## Configuring Miscellaneous Online Charging Trigger Events

As a part of the online trigger profile configuration, you can configure the following miscellaneous attributes:

- Grace quota to be granted in case of credit control failure
- Default measurement method to be used
- Quota holding time
- Quota threshold
- Quota validity time
- Reporting level
- Attributes (including quotas) for the requested service unit

To configure the miscellaneous attributes:

1. Configure the grace quota. The broadband gateway allocates the grace quota in case of credit control failure; for example, if there is no reply from the OCS to the CCR message.

- a. Configure the volume quota (in bytes) for both uplink and downlink directions.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online]
user@host# set grant-quota cc-octet-both volume-quota-both
```

The range for the volume quota for both the uplink and downlink directions is 1,048,576 through 9,223,372,036,854,775,807 bytes.

- b. Configure the volume quota (in bytes) for the downlink direction.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online]
user@host# set grant-quota cc-octet-downlink volume-quota-dl
```

The range for the volume quota for in the downlink direction is 1,048,576 through 9,223,372,036,854,775,807 bytes.

- c. Configure the volume quota (in bytes) for the uplink direction.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online]
user@host# set grant-quota cc-octet-uplink volume-quota-ul
```

The range for the volume quota for in the downlink direction is 1,048,576 through 9,223,372,036,854,775,807 bytes.

- d. Configure the time quota (in seconds).

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online]
user@host# set grant-quota cc-time time-quota
```

The range for the time quota is 300 through 4,294,967,294 seconds.

2. Specify the default measurement method to be used. This specified measurement method is used by the gateway to include the Requested-Service-Unit (RSU) AVP in the CCR message if the policy and charging enforcement function (PCEF) does not include the RSU AVP in the CCR message.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online]
user@host# set measurement-method (none | time | volume | volume-and-time)
```

If you specify **time** as the default measurement method, then the gateway includes the CC Time AVP in the RSU based on configured time (**cc-time** statement). If you specify **volume** as the default measurement method, the gateway includes the CC Octet Both, CC Octet Downlink, and CC Octet Uplink AVPs in the RSU based on configured values (**cc-octet-both**, **cc-octet-downlink**, and **cc-octet-uplink** statements, respectively). If you specify **volume-and-time**, then the gateway includes both time and volume AVPs in the RSU. If you specify **none**, then the gateway sends an empty RSU.

3. Configure the quota holding time, in seconds. The configured quota holding time is used if the OCS does not provide quota validity time in the Quota-Holding-Time AVP in the Credit Control Answer (CCA) message.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online]
user@host# set quota-holding-time time-in-seconds
```

The range for the quota holding time is 300 through 864,000 seconds.



**NOTE:** The quota holding time provided by the OCS takes precedence over the one configured (locally) on the broadband gateway. A quota holding time of zero indicates that the quota holding mechanism should not be used.

If you do not include the `quota-holding-time` statement, the quota holding time provided by the OCS is used. If no quota holding time is provided by the OCS, then the quota holding mechanism is not used.

4. Configure the threshold for the quota received from the OCS:
  - a. Specify the quota threshold as a percentage of the total quota allocated. The broadband gateway uses the quota threshold to determine when to report the used quota to and request more quota from the OCS. For example, if the OCS provides 100 KB of quota and if the quota threshold is 80 percent, then the gateway sends the OCS a Credit Control Request-Update message with the used quota, when the quota used is 80 KB.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online]
user@host# set quota-threshold threshold
```

The range for the quota threshold is 5 through 95 percent.

- b. Optionally, specify that the configured quota threshold overrides the one provided by the OCS.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online]
user@host# set quota-threshold override
```

5. Configure the quota validity time, in seconds. The configured quota validity time is used if the OCS does not provide quota validity time in the Validity-Time AVP in the Credit Control Answer (CCA) message.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online]
user@host# set quota-validity-time time-in-seconds
```

The range for the quota validity time is 30 through 864,000 seconds.

6. Configure the default reporting level for the reports from the gateway to the offline charging gateway and the OCS:
  - a. Specify the reporting level. You can specify whether the gateway reports at the rating group level or at the service identifier level (within a rating group).



```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online]
```

```
user@host# set reporting-level (rating-group | service-identifier)
```

- b. Optionally, specify that the configured reporting level overrides the one provided by the PCRF.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online]
```

```
user@host# set reporting-level override
```

7. Configure the attributes for the requested service unit. (The broadband gateway uses the configured quotas in the RSU AVP in the CCR message to the OCS.)

- a. Specify that the broadband gateway always includes the RSU AVP in CCR messages to the OCS.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online]
```

```
user@host# set requested-service-unit always-include
```



**NOTE:** By default, the broadband gateway includes the RSU AVP in CCR messages sent to the OCS requesting for quota, except in the following cases:

- If the quota holding time has elapsed, the broadband gateway returns the quota to the OCS and does not request for more quota.
- If the `send-ccri-on-first-packet` statement has not been included, and if the `quota-request-on-first-packet` statement is configured, the broadband gateway sends a CCR-I message to the OCS, to authorize the bearer, without the RSU AVP included.

- b. Specify that the broadband gateway includes the RSU AVP in the CCR messages to the OCS, when the usage is reported for the reason of quota holding time.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online]
```

```
user@host# set requested-service-unit include-quota-holding-time
```



**NOTE:**

- By default, the gateway does not include the RSU AVP in CCR messages to the OCS, when the reporting reason is quota holding time.
- If you configure both the `always-include` and `include-quota-validity-time` statements, the `always-include` statement takes precedence.

- c. Configure the volume quota (in bytes) for both uplink and downlink directions.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online]
```

```
user@host# set requested-service-unit cc-octet-both volume-quota-both
```

The range for the volume quota for both the uplink and downlink directions is 1,048,576 through 9,223,372,036,854,775,807 bytes.

- d. Configure the volume quota (in bytes) for the downlink direction.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online]
```

```
user@host# set requested-service-unit cc-octet-downlink volume-quota-dl
```

The range for the volume quota for in the downlink direction is 1,048,576 through 9,223,372,036,854,775,807 bytes.

- e. Configure the volume quota (in bytes) for the uplink direction.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online]
```

```
user@host# set requested-service-unit cc-octet-uplink volume-quota-ul
```

The range for the volume quota for in the downlink direction is 1,048,576 through 9,223,372,036,854,775,807 bytes.

- f. Configure the time quota (in seconds).

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online]
```

```
user@host# set requested-service-unit cc-time time-quota
```

The range for the time quota is 300 through 4,294,967,294 seconds.

- g. Specify that the broadband gateway includes the Requested-Service-Unit AVP in the CCR messages to the OCS, when the usage is reported for the reason of quota holding time.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
online]
```

```
user@host# set requested-service-unit include-quota-holding-time
```



**NOTE:** By default, the gateway does not include the Requested-Service-Unit AVP in CCR messages to the OCS, when the reporting reason is quota holding time.

---

#### Related Documentation

- [Configuring Charging Profiles on page 467](#)
- [Example: Configuring Online Charging on page 486](#)
- [online \(Trigger Profiles\)](#)
- [Online Charging Overview on page 433](#)
- [Tracing Charging Operations on page 470](#)
- [trigger-profiles \(GGSN or P-GW\)](#)

---

## Verifying and Managing the Charging Configuration

|                |                                                                |
|----------------|----------------------------------------------------------------|
| <b>Purpose</b> | Display or clear information about the charging configuration. |
|----------------|----------------------------------------------------------------|



**NOTE:** This topic lists commands that are applicable only to the Gateway GPRS Support Node (GGSN) or Packet Data Network Gateway (P-GW). However, you can display or clear information about the charging configuration for the Serving Gateway (S-GW). Replace the `ggsn-pgw` keyword in the commands below with `sgw` to run the corresponding commands for the S-GW; for example, `show unified-edge sgw charging local-persistent-storage statistics` displays information about the local persistent storage statistics on the S-GW.

- Action**
- To display information about the local persistent storage statistics:  
`user@host> show unified-edge ggsn-pgw charging local-persistent-storage statistics`
  - To display information about the path management message statistics:  
`user@host> show unified-edge ggsn-pgw charging path statistics`
  - To display information about the status of the configured peers:  
`user@host> show unified-edge ggsn-pgw charging path status`
  - To display information about the transfer statistics for configured transport profiles:  
`user@host> show unified-edge ggsn-pgw charging transfer statistics`
  - To display information about the transfer status for configured transport profiles:  
`user@host> show unified-edge ggsn-pgw charging transfer status`
  - To clear the locally-stored CDRs:  
`user@host> clear unified-edge ggsn-pgw charging cdr`
  - To clear the local persistent storage statistics:  
`user@host> clear unified-edge ggsn-pgw charging local-persistent-storage statistics`
  - To clear the path management message statistics:  
`user@host> clear unified-edge ggsn-pgw charging path statistics`
  - To clear the transfer statistics:  
`user@host> clear unified-edge ggsn-pgw charging transfer statistics`

- Related Documentation**
- [Configuring Persistent Storage on page 455](#)
  - [Configuring GTP Prime for Charging on page 453](#)
  - [Configuring Transport Profiles for Offline Charging on page 459](#)
  - [Configuring Charging Trigger Events for Offline Charging on page 462](#)
  - [Configuring S-GW-Specific Charging Parameters on page 444](#)
  - [Configuring S-GW Global Charging Profiles and Selection Order on page 446](#)
  - [Configuring S-GW Charging Traceoptions on page 448](#)

## Example: Configuring Online Charging

---

This example shows how to configure the MobileNext Broadband Gateway so that charging is carried out online in real time. By default, the broadband gateway records no charging information. The broadband gateway conveys online charging information to the Online Charging Server (OCS) over the Gy interface using the Diameter protocol.

- [Requirements on page 486](#)
- [Overview on page 486](#)
- [Configuration on page 487](#)
- [Verification on page 491](#)
- [Troubleshooting on page 492](#)

### Requirements

This example uses the following hardware and software components:

- A supported MX Series chassis configured with supported line cards and a services PIC.
- A supported and properly installed version of 64-bit Junos OS and the **jmobile** software package.
- Correct configuration as a Packet Data Network Gateway (P-GW) with corresponding interfaces.

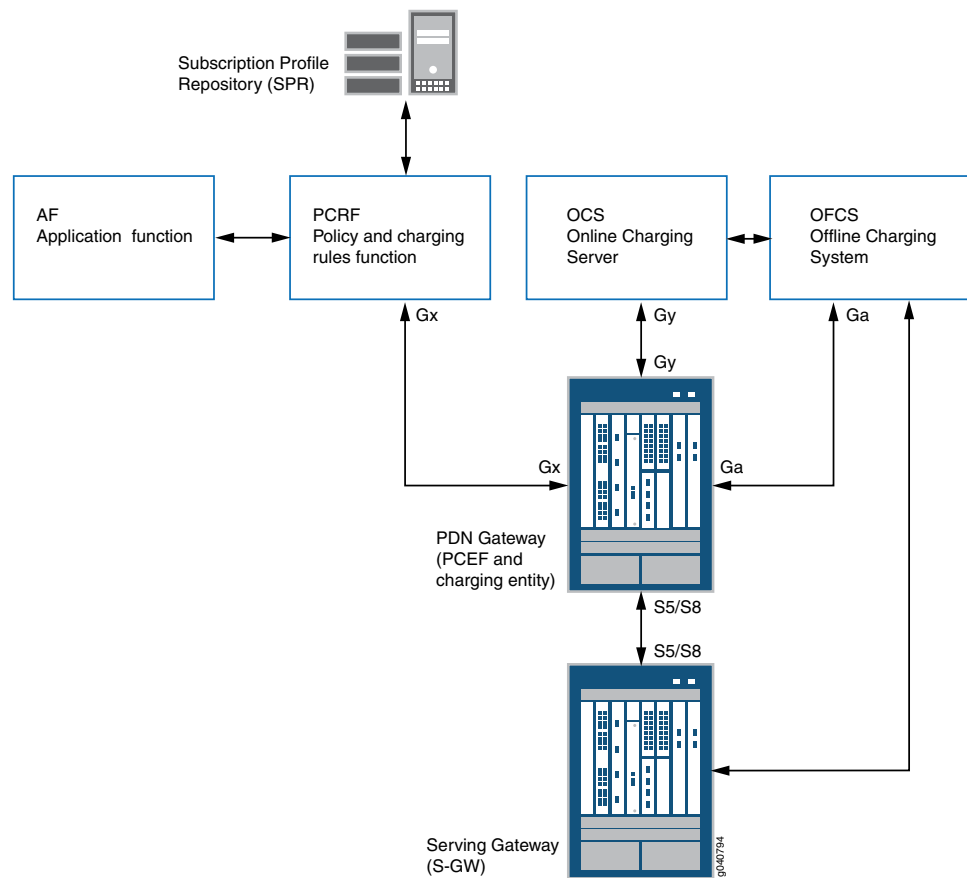
Before you configure online charging, be sure you have:

- Configured the broadband gateway correctly.
- Configured GTP and Diameter correctly.

### Overview

Online charging is part of a complete broadband gateway configuration, including policy and charging rules, quality-of-service (QoS) determination, and overall charging considerations. [Figure 56 on page 487](#) shows the overall architecture for the gateway components and the functional groupings for policy and charging. The Gy interface connects the P-GW and OCS.

Figure 56: Architecture for Online Charging



You can configure both online and offline charging. This example configures only online charging, including the Gy interface.

### Topology

The topology for this online charging example consists of mobile network nodes and the interfaces connecting them to each other. The key device is the P-GW, which incorporates the charging entity to handle charging information, and the policy and charging enforcement functions (PCEF) to determine how the charging and policy information is handled. The P-GW communicates with the OCS over the Gy interface, which is the main interface configured for online charging.

### Configuration

To configure online charging, perform these tasks:

- [Configuring Online Charging on page 488](#)
- [Results on page 490](#)

#### CLI Quick Configuration

```
set unified-edge gateways ggsn-pgw mbg-1 charging trigger-profiles trigger-profile-1
  tariff-time-list 17:00:00
set unified-edge gateways ggsn-pgw mbg-1 charging trigger-profiles trigger-profile-1
  tariff-time-list 18:00:00
```

```

set unified-edge gateways ggsn-pgw mbg-1 charging trigger-profiles trigger-profile-1
  tariff-time-list 20:05:00
set unified-edge gateways ggsn-pgw mbg-1 charging trigger-profiles trigger-profile-1
  tariff-time-list 22:05:00
set unified-edge gateways ggsn-pgw mbg-1 charging trigger-profiles trigger-profile-1
  online quota-threshold 80
set unified-edge gateways ggsn-pgw mbg-1 charging trigger-profiles trigger-profile-1
  online grant-quota cc-octet-both 5000000
set unified-edge gateways ggsn-pgw mbg-1 charging trigger-profiles trigger-profile-1
  online requested-service-unit cc-time 1800
set unified-edge gateways ggsn-pgw mbg-1 charging trigger-profiles trigger-profile-1
  online requested-service-unit cc-octet-both 1048576
set unified-edge gateways ggsn-pgw mbg-1 charging trigger-profiles trigger-profile-1
  online cc-failure-handling update-request convert-to-offline
set unified-edge gateways ggsn-pgw mbg-1 charging transport-profiles transport-profile-1
  online tx-timeout 5
set unified-edge gateways ggsn-pgw mbg-1 charging transport-profiles transport-profile-1
  online session-failover-not-supported
set unified-edge gateways ggsn-pgw mbg-1 charging transport-profiles transport-profile-1
  online diameter-profile gy-profile-1
set unified-edge gateways ggsn-pgw mbg-1 charging transport-profiles transport-profile-1
  online send-ccri-on-first-packet
set unified-edge gateways ggsn-pgw mbg-1 charging transport-profiles transport-profile-1
  online set-quota-request-on-first-packet
set unified-edge gateways ggsn-pgw mbg-1 charging charging-profiles
  default-charging-profile profile-id 232
set unified-edge gateways ggsn-pgw mbg-1 charging charging-profiles
  default-charging-profile transport-profile transport-profile-1
set unified-edge gateways ggsn-pgw mbg-1 charging charging-profiles
  default-charging-profile trigger-profile trigger-profile-1 rating-group 1000

```

## Configuring Online Charging

### Step-by-Step Procedure

To configure online charging on the broadband gateway:



**NOTE:** You can configure both offline and online charging parameters and profiles. This example only configures online charging parameters and profiles.

1. Enable online charging at the PCEF level if using static policies.

[edit]

```

user@mbg# set unified-edge gateways ggsn-pgw mbg-1 pcef static-policies
pcc-rules pcc-rule-1 charging charging-method online

```



**NOTE:** You can also set the charging-method to online-offline to enable online charging. If you do not include this statement in the rule, the default is to apply the bearer-level charging method, which could be none (no charge).

2. Enable online charging at the bearer (trigger profile) level if not using charging in a static policy.

[edit]

```
user@mbg# set unified-edge gateways ggsn-pgw mbg-1 charging trigger-profiles
trigger-profile-1 charging-method online
```



**NOTE:** This establishes the default charging method if the PCEF static policy does not provide a method.

3. Configure trigger profiles for online charging parameters.

[edit]

```
user@mbg# set unified-edge gateways ggsn-pgw mbg-1 charging trigger-profiles
trigger-profile-1 tariff-time-list 17:00:00
user@mbg# set unified-edge gateways ggsn-pgw mbg-1 charging trigger-profiles
trigger-profile-1 tariff-time-list 18:00:00
user@mbg# set unified-edge gateways ggsn-pgw mbg-1 charging trigger-profiles
trigger-profile-1 tariff-time-list 20:05:00
user@mbg# set unified-edge gateways ggsn-pgw mbg-1 charging trigger-profiles
trigger-profile-1 tariff-time-list 22:05:00
user@mbg# set unified-edge gateways ggsn-pgw mbg-1 charging trigger-profiles
trigger-profile-1 online quote-threshold 80
user@mbg# set unified-edge gateways ggsn-pgw mbg-1 charging trigger-profiles
trigger-profile-1 online grant-quota cc-octet-both 5000000
user@mbg# set unified-edge gateways ggsn-pgw mbg-1 charging trigger-profiles
trigger-profile-1 online quote-threshold 80
user@mbg# set unified-edge gateways ggsn-pgw mbg-1 charging trigger-profiles
trigger-profile-1 online requested-service-unit cc-time 1800
user@mbg# set unified-edge gateways ggsn-pgw mbg-1 charging trigger-profiles
trigger-profile-1 online requested-service-unit cc-octet-both 1048576
user@mbg# set unified-edge gateways ggsn-pgw mbg-1 charging trigger-profiles
trigger-profile-1 online cc-failure-handling update-request convert-to-offline
```



**NOTE:** You configure a list of local tariff times (in hh, hh:mm, or hh:mm:ss format) at which the tariff changes and Charging Data Records (CDRs) are generated to reflect the change in tariff. Make sure that there is a difference of at least 15 minutes between multiple values. The seconds values are ignored. You can configure a maximum of 24 values. The local time zone's Universal Metric Time (UMT) offset is added to the time configured.

4. Configure transport profiles for online charging parameters.

[edit]

```
user@mbg# set unified-edge gateways ggsn-pgw mbg-1 charging transport-profiles
transport-profile-1 online tx-timeout 5
user@mbg# set unified-edge gateways ggsn-pgw mbg-1 charging transport-profiles
transport-profile-1 online session-failure-not-supported
```

```

user@mbg# set unified-edge gateways ggsn-pgw mbg-1 charging transport-profiles
transport-profile-1 online diameter-profile gy-profile-1
set unified-edge gateways ggsn-pgw mbg-1 charging transport-profiles
transport-profile-1 online send-ccri-on-first-packet
set unified-edge gateways ggsn-pgw mbg-1 charging transport-profiles
transport-profile-1 online set-quota-request-on-first-packet

```



**NOTE:** The Diameter profile must be properly configured under the Diameter configuration.

5. Configure charging profiles for online charging parameters.

```

[edit]
user@mbg# set unified-edge gateways ggsn-pgw mbg-1 charging charging-profiles
default-charging-profile profile-id 232
user@mbg# set unified-edge gateways ggsn-pgw mbg-1 charging charging-profiles
default-charging-profile transport-profile transport-profile-1
user@mbg# set unified-edge gateways ggsn-pgw mbg-1 charging charging-profiles
default-charging-profile trigger-profile trigger-profile-1 rating-groups 1000

```

## Results

From configuration mode, confirm your configuration by entering the **show** command at the correct hierarchy level. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

For brevity, this **show** command output includes only the configuration that is relevant to this example.

```

[edit unified-edge gateways ggsn-pgw mbg-1 charging]
trigger-profiles {
  trigger-profile-1 {
    tariff-time-list {
      "17:00:00 -0700";
      "18:00:00 -0700";
      "20:05:00 -0700";
      "22:05:00 -0700";
    }
    online {
      quota-threshold 80;
      grant-quota {
        cc-octet-both 5000000;
      }
      requested-service-unit {
        cc-time 1800;
        cc-octet-both 1048576;
      }
      cc-failure-handling {
        update-request {
          convert-to-offline;
        }
      }
    }
  }
}

```



```

    }
  }
}
transport-profiles {
  transport-profile-1 {
    online {
      tx-timeout 5;
      session-failover-not-supported;
      diameter-profile gy-profile-1;
      quota-request-on-first-packet;
      send-ccri-on-first-packet;
    }
  }
}
charging-profiles {
  default-cp {
    profile-id 232;
    transport-profile transport-profile-1;
    trigger-profile trigger-profile-1 {
      rating-group 1000;
    }
  }
}
}

```

## Verification

### Verifying Online Charging Peer Status Configuration

- Purpose** Verify that the online charging peer is successfully communicating with the broadband gateway.
- Action** From operational mode, enter the **show unified-edge ggsn-pgw diameter peer status detail** command.
- ```

user@mgb-1# show unified-edge ggsn-pgw diameter peer status
Diameter Peer Status
  Name : p1
    FPC/PIC           :          3/0
    State              :          I-Open
    State Duration     :          00:01:31
    Watchdog State     :          okay
    Origin Host        :          mydomain.net
    Origin Realm       :          mydomain.net
    Peer Address       :          10.6.1.2
    Peer port          :          3868
    Source Address     :          10.6.88.1
    Source Port        :          30736
  
```
- Meaning** If the output shows that the state of the peer is “I-Open,” then the connection to the OCS is established.

### Verifying Online Charging Peer Statistics

- Purpose** Verify that the online charging peer is successfully sending to and receiving from the broadband gateway.
- Action** From operational mode, enter the **show unified-edge ggsn-pgw diameter dcca-gy statistics detail** command.
- ```
user@mgb-1# show unified-edge ggsn-pgw diameter dcca-gy statistics detail
```
- Gateway: PGW  
FPC/PIC: 3/0
- |                            |   |  |  |  |
|----------------------------|---|--|--|--|
| Total Sessions:            | 1 |  |  |  |
| Total Sessions Terminated: | 0 |  |  |  |
| Internal Errors:           | 0 |  |  |  |
- 
- | Credit Control              | Initial | Update | Terminate | Total |
|-----------------------------|---------|--------|-----------|-------|
| -----                       |         |        |           |       |
| Requests Transmitted        | 1       | 0      | 1         | 2     |
| Request Timeouts            | 0       | 0      | 0         | 0     |
| Request Tx Timeouts         | 0       | 0      | 0         | 0     |
| Request Discarded           | 0       | 0      | 0         | 0     |
| Answers Received            | 1       | 0      | 1         | 2     |
| Answers Dropped             | 0       | 0      | 0         | 0     |
| Answers Parse Errors        | 0       | 0      | 0         | 0     |
| Answers with Invalid AVP(s) | 0       | 0      | 0         | 0     |
- 
- | Server Requests              | Re-Auth | Abort Session | Total |
|------------------------------|---------|---------------|-------|
| -----                        |         |               |       |
| Requests Received            | 0       | 1             | 1     |
| Requests Dropped             | 0       | 0             | 0     |
| Requests Parse Errors        | 0       | 0             | 0     |
| Requests with Invalid AVP(s) | 0       | 0             | 0     |
| Answers Transmitted          | 0       | 1             | 1     |
- Meaning** If the output shows that the number of requests transmitted and answers received is non-zero, then the connection to the OCS is functioning properly.

## Troubleshooting

To troubleshoot online charging configuration, perform these tasks:

- [Troubleshooting Rating Group and Volume Quota on page 492](#)

### Troubleshooting Rating Group and Volume Quota

- Problem** The rating group and quota granted by the OCS is not as expected for the subscriber.
- Solution** To display the rating group for online charging and the quota for the subscriber, perform the following:
1. From operational mode, enter the **show unified-edge ggsn-pgw subscribers extensive** command.

```
user@mgb-1# show unified-edge ggsn-pgw subscribers extensive
Gateway: PGW
```

Subscriber Information:

UE:

```
IMSI: 223456789012369      IMEI: 3568710407092001
MSISDN: 62818881442      Time Zone: GMT      DST: None
RAT Type: UTRAN
User Location Information:
MCC: None  MNC: None
LAC: 0x0  CI: 0x0      SAC: 0x0  RAC: 0x0  TAC: 0x0  ECI: 0x0
```

PDN Session:

APN name: jnpr-gxgy

```
IPv4 Address: 30.30.0.1      IPv6 Address: None
GTP Version: 1      Address Assignment: Local
```

```
Local Control IP: 200.6.88.1      Remote Control IP: 70.70.70.4
Local Control TEID: 0x12000000      Remote Control TEID: 0x1
Selection mode: MS or network provided APN, subscription verified
```

```
Session PIC: 0 /0 (FPC/PIC)      PFE: 2 /0 (FPC/PIC)
Service PIC: None/None (FPC/PIC)
Session State: Established      Session Duration: 8
Roaming Status: Visitor      Serving network: MCC: 123  MNC: 456
Direct Tunnel: Disabled
HW Rule set Identifier: 0      Rule Map: 1
PCRF Event Triggers: QoS |TIMEOUT
```

PCRF Origin Host: diameter1

PCRF Origin Realm: hitachi.com

Usage Monitoring Information:

Monitoring Key: 0

```
Status: 2000      Total: Active
```

Bearer:

```
NSAPI/EBI: 5
Local Data IP: 200.6.88.1      Remote Data IP: 70.70.70.4
Local Data TEID: 0x14120000      Remote Data TEID: 0x1001
Bearer State: Established
Idle Timeout: 0 min      AAA Interim Interval: 0 min
QoS Parameters:
Traffic Class: Interactive      ARP: 3
Traffic Handling Priority: 1      Transfer Delay: 0
MBR Uplink: 1664 kbps      MBR Downlink: 1664 kbps
Signaling Indicator: 0
Forwarding Class: None      Loss Priority: None
```

Mapped V2 Parameters:

```
QCI: 6      ARP: 11/1 /1 (PL/PVI/PCI)
```

Charging information:

```
Charging ID: 0x12000000      Transport Profile Name: tp1
Charging Characteristics: 0x8
Profile ID: 1      Charging Profile name: cp1
State: Ready      Previous State: None
```

Profile selection criteria: Static default

Details: Offline, Online

Statistics information (PFE cleared and non-cleared): None collected

```
Offline charging information:
  Current service data container sequence number: None
  Current partial record sequence number:          1
  Number of CDRs closed:                          0
  Number of containers closed:                     0
Online charging information:
  Number of online rating groups: 1 Next CC request number: 1
  CC Failure Handling: Retry-and-Terminate Last CCR result code: 2001
Rating group information:
  Rating group: 100 Service id: 2 State: Ready
  RG Action ID: 0x2020000 Trigger profile: trp1
  Details: Offline RG, Online RG
  Reporting Level: Rating Group
  Volume Quota: Total: 3000 Uplink: 1500 Downlink: 1500
                  Holding time: 600
                  Collection time: Fri Feb  8 06:56:56 2013
                  Uplink packets: 0 Downlink packets : 0
                  Uplink bytes: 0 Downlink bytes : 0
PCC Rule Information:
Rule Name: gx-rule-2
  Type: Static Associated Rule Base: None
  Precedence: 100 Status: Active
QoS Attributes:
  QCI: 6 ARP: 11/0 /0 (PL/PVI/PCI)
Charging Attributes:
  Rating Group: 100 Service ID: 2 Gating Status: enable-both
  AF Charging Id: None Charging Method: Online-Offline Metering Method:
None
  Usage Monitoring Key : NULL
Filter Attributes:
  Remote IP/Mask: 200.6.1.2/32 Protocol: any Direction: Both
  Local Ports: any
  Remote Ports: any
  Send to UE: Yes
```

- 
2. The rating group reporting level for online charging for the subscriber is displayed under **Rating group information** in the output. Make sure that the reporting level is correct.
3. The volume quota uplink and downlink and total is displayed under **Rating group information** in the output. Make sure that the quotas are correct.

#### Related Documentation

- [Charging Overview on page 429](#)
- [Configuring Offline Charging on page 443](#)
- [Configuring Charging Profiles on page 467](#)
- [Configuring Transport Profiles for Offline Charging on page 459](#)
- [Configuring Charging Trigger Events for Offline Charging on page 462](#)
- [Configuring CDR Attributes on page 464](#)
- [Configuring Charging Profiles for APNs on page 469](#)

## Configuring Service Sets and Service Filters for Advice of Charge

The Advice of Charge (AoC) feature provides a subscriber with information about any applicable charges *before* the subscriber uses a service, or when the subscriber's quota is exhausted. The service set and services filter names are variables, but must conform to the usual Junos OS naming rules.

Before you begin configuring a service set and service filter for AoC and top-up on a broadband gateway, you should have done the following:

- Configured the chassis of the broadband gateway
- Configured the interfaces of the broadband gateway
- Configured a zero-rated or unlimited rating group to allow the “redirect-URL” traffic towards the AoC or top-up server.

To configure the AoC service set and service filter and apply them to the mobile interface of the APN:

1. Configure a policy and charging enforcement function (PCEF) profile. (The name *aoc\_pcef* is a variable.)

```
[edit services]
user@mbg# set pcef profile aoc_pcef
```

2. Configure the service set for AoC. (The name *aoc\_service\_set* is a variable.)

```
[edit services service-set aoc_service_set]
user@mbg# set tcp-mss 1300
user@mbg# set service-set-options subscriber-awareness
```

3. Reference the configured PCEF profile in a service set. (The name *profile1* is a variable.)

```
[edit services service-set aoc_service_set]
user@mbg# set application-identification-profile profile1
user@mbg# set pcef-profile aoc_pcef
user@mbg# set interface-service service-interface ams0.1
user@mbg# set interface-service load-balancing options hash-keys resource-triggered
```



**NOTE:** The PCEF profile referenced is the PCEF profile configured at the [edit services pcef] hierarchy level.

4. Configure the AoC service filter. There is only one term in this filter that selects packets for AoC and top-up servicing. (The term *aoc\_filter* is a variable.)

```
[edit firewalls family inet service-filter aoc_filter term t1]
user@mbg# set from redirect-reason [ dpi aoc ]
user@mbg# set then service
```



**NOTE:** You must include deep packet inspection (DPI) as well as AoC as the redirect reason for this feature to function properly.

5. Apply the previously configured AoC service set and service filter for input and output on the mobile interface (**mif.0**) of the APN.

```
[edit interfaces mif unit 0 family inet]
user@mbg# set service input service-set aoc_service_set service-filter aoc_filter
user@mbg# set service output service-set aoc_service_set service-filter aoc_filter
```

---



**NOTE:** The service set referenced must be configured at the [edit services service-set] hierarchy level, and the service filter referenced must be configured at the [edit firewall family inet service-filter] hierarchy level.

---

**Related  
Documentation**

- [Advice of Charge Overview on page 440](#)
- [Service Sets and Service Filters for Advice of Charge Overview on page 441](#)
- [Configuring Policy and Charging Control Action Profiles on page 369](#)
- [Configuring Application-Aware Policy and Charging Control Rules on page 371](#)
- [Example: Configuring Policy and Charging Enforcement Function with Application-Aware Policy and Charging Control Rules on page 397](#)

## PART 9

# Quality of Service Configuration

- [Quality of Service Overview on page 499](#)
- [Configuring Quality of Service on page 515](#)





## CHAPTER 21

# Quality of Service Overview

- [Quality of Service Overview on page 499](#)
- [Call Admission Control Overview on page 506](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 508](#)
- [Policing Subscriber Traffic on the Broadband Gateway Overview on page 509](#)
- [Applying Rewrite Rules on Mobile Interfaces Overview on page 510](#)
- [Understanding Upstream and Downstream Processing of ToS Values in GTP-U Packets on page 511](#)
- [Understanding How NQN and Upgrade Flags in PDP Contexts Affect QoS Upgrade Behavior on page 513](#)

## Quality of Service Overview

---

Quality of service (QoS) allows both subscribers and services to be differentiated. Premium subscribers can be prioritized over basic subscribers, while real-time services can be prioritized over non-real-time services. The importance of QoS increases during periods of congestion. An unloaded network can meet the needs of all subscribers and services. However, as the network load increases, the prioritization of traffic determines whether performance for subscribers and services can be maintained or will be degraded.

In a mobile network, network resources are shared among multiple services (including Internet, voice, video, e-mail, and file sharing), each of which has different QoS requirements in terms of required bit rates, acceptable packet loss rates, and packet delay. On the MobileNext Broadband Gateway, you configure QoS profiles and policies to define the QoS treatment for mobile subscribers in 3G and 4G networks.

This topic covers:

- [Initial QoS on page 500](#)
- [Differentiated Services on page 500](#)
- [QoS Parameters in 3G Networks on page 500](#)
- [Default Conversion of \(3G\) Traffic Classes to \(4G\) QoS Class Identifiers on the Broadband Gateway on page 502](#)
- [QoS Parameters in 4G Networks on page 503](#)
- [Aggregate Maximum Bit Rate on page 504](#)

- [Allocation and Retention Priority on page 504](#)
- [Preemption on page 505](#)

## Initial QoS

When a bearer is first established on the broadband gateway, an initial level of QoS is assigned to the bearer based on QoS attributes in the QoS information element (IE) that specify the traffic characteristics for a bearer. Traffic characteristics include delay class, reliability class, precedence class, and traffic class or traffic handling priority (3G subscribers) or QoS Class Identifier (QCI) (4G subscribers).



**NOTE:** For 3G subscribers, the broadband gateway converts the traffic class to a QCI based on the 3GPP specification 23.401 ANNEX E. For more information, see [“QoS Parameters in 3G Networks” on page 500](#).

## Differentiated Services

The broadband gateway supports QoS using the Differentiated Services (DiffServ) model. The DiffServ model is a multiple-service model that addresses different QoS requirements. With DiffServ, the network tries to deliver a particular kind of service based on the QoS specified by each packet, for example, using the 6-bit DiffServ code point (DSCP) setting in IP packets.

Standards for Differentiated Services are described in the following documents:

- RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*
- RFC 2475, *An Architecture for Differentiated Services*

## QoS Parameters in 3G Networks

In a 3G network, subscriber traffic is classified based on traffic classes. Each traffic class is associated with a maximum bit rate and (for GBR bearers) a guaranteed bit rate, which can be configured independently for uplink and downlink subscriber traffic. To define the packet-forwarding treatment for bearer requests received on the broadband gateway, you configure a QoS classifier profile to map each traffic class (and for the Interactive class, traffic class, and traffic handling priority) to a forwarding class and packet loss priority (PLP).



**NOTE:** If no classifier profile is configured on the broadband gateway to map the traffic classes to a forwarding class and packet loss priority, the classification specified in the bearer request, coming from either the Gn or Gi interface, is carried over.

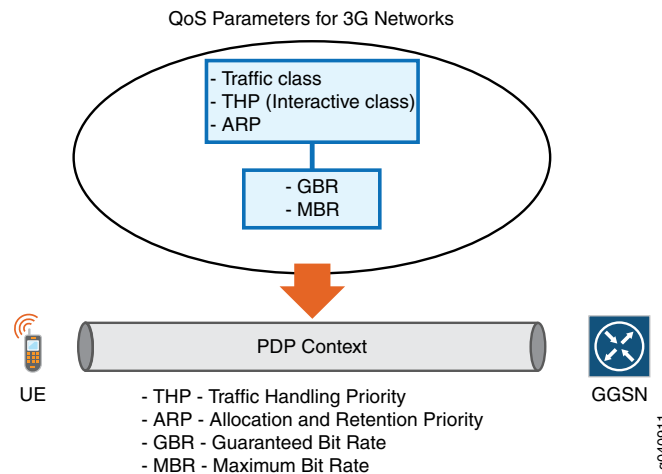
[Table 54 on page 501](#) shows the supported traffic classes, as defined in the 3GPP standards.

Table 54: Traffic Classes for 3G Networks

| Traffic Class  | Description                                                                                                                                                                                                                                   | Example Services                                                               |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| Conversational | Conversational pattern with very low delay and jitter. This is the most delay-sensitive traffic class.                                                                                                                                        | Voice and real-time multimedia messaging such as VoIP and video conferencing.  |
| Streaming      | Delay and jitter requirements are not as strict as with conversational traffic class.                                                                                                                                                         | Streaming type applications such as video on demand.                           |
| Interactive    | Interactive class enables prioritization between packet data protocol (PDP) contexts, which allows end-user or service prioritization. Interactive class is associated with a traffic handling priority (THP). THP values can be 1 through 3. | Streaming type applications such as video on demand, Web browsing, and Telnet. |
| Background     | Best effort is acceptable for data delivery. This is the least delay-sensitive traffic class.                                                                                                                                                 | Background type applications such as e-mail and FTP.                           |

A policy profile defines the QoS treatment to apply for each traffic class or traffic handling priority. [Figure 57 on page 501](#) shows the QoS parameters that the broadband gateway evaluates to determine whether to limit, upgrade, or reject an incoming PDP context request.

Figure 57: Key QoS Parameters for PDP Context Requests



The guaranteed bit rate (GBR), shown in [Figure 57 on page 501](#), defines the minimum bit rate that is expected to be available to the PDP context when required. The GBR signifies that a certain amount of bandwidth is reserved for the PDP context, regardless of whether or not the GBR is used. Consequently, a PDP context with a GBR always takes up resources even when no traffic is forwarded. Under normal operating conditions, the PDP context should not experience any packet loss due to congestion on the network. This is ensured because the PDP context is subject to admission control during initial setup, and a network allows the PDP context with a GBR only if sufficient resources are available. You can specify the GBR independently for uplink and downlink traffic.

The maximum bit rate (MBR), shown in [Figure 57 on page 501](#), defines the maximum bit rate that is expected to be available to the PDP context when required. An MBR limits

the bit rate that will be provided to a PDP context. Any traffic that exceeds the MBR can be dropped. You can specify the MBR independently for uplink and downlink traffic.

## Default Conversion of (3G) Traffic Classes to (4G) QoS Class Identifiers on the Broadband Gateway

For 3G subscribers, the broadband gateway converts the traffic class to a QCI, based on the 3GPP specification 23.401 ANNEX E. [Table 55 on page 502](#) shows the mapping between standardized QCI values and the Release 99 (GTPv1) QoS parameters.

**Table 55: Mapping of Traffic Classes to Qos Class Identifiers**

| QCI | Traffic Class  | Traffic Handling Priority | Signaling Indication | Source Statistics Descriptor                                                                                                                                                                                                                                                                                                                                 |
|-----|----------------|---------------------------|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | Conversational | N/A                       | N/A                  | Speech.                                                                                                                                                                                                                                                                                                                                                      |
| 2   | Conversational | N/A                       | N/A                  | Unknown.<br><br><b>NOTE:</b> When QCI 2 is mapped to pre-Release 8 QoS parameter values, the Transfer Delay parameter is set to 150 ms. When pre-Rel-8 QoS parameter values are mapped to a QCI, QCI 2 is used for conversational/unknown if the Transfer Delay parameter is greater or equal to 150 ms.                                                     |
| 3   | Conversational | N/A                       | N/A                  | Unknown.<br><br><b>NOTE:</b> When QCI 3 is mapped to pre-Release 8 QoS parameter values, the Transfer Delay parameter is set to 80 ms as the lowest possible value, according to TS 23.107 [54]. When pre-Release 8 QoS parameter values are mapped to a QCI, QCI 3 is used for conversational/unknown if the Transfer Delay parameter is lower than 150 ms. |
| 4   | Streaming      | N/A                       | N/A                  | Unknown.<br><br><b>NOTE:</b> When QCI 4 is mapped to pre-Release 8 QoS parameter values, it is mapped to Streaming/Unknown. When pre-Release 8 QoS parameter values are mapped to a QCI, Streaming/Unknown and Streaming/Speech are both mapped to QCI 4.                                                                                                    |
| 5   | Interactive    | 1                         | Yes                  | N/A                                                                                                                                                                                                                                                                                                                                                          |
| 6   | Interactive    | 1                         | No                   | N/A                                                                                                                                                                                                                                                                                                                                                          |
| 7   | Interactive    | 2                         | No                   | N/A                                                                                                                                                                                                                                                                                                                                                          |
| 8   | Interactive    | 3                         | No                   | N/A                                                                                                                                                                                                                                                                                                                                                          |
| 9   | Background     | N/A                       | N/A                  | N/A                                                                                                                                                                                                                                                                                                                                                          |

## QoS Parameters in 4G Networks

In a 4G network, subscriber traffic is classified based on the QoS Class Identifier (QCI), which is associated with priority, specify delay, and packet loss values, and determines the user plane treatment for IP packets transported on a bearer. The QCI determines which bearers are categorized as GBR (dedicated) and which are categorized as non-GBR (default). The broadband gateway supports only default bearers, which correspond to QCI values 5 through 9. The broadband gateway does not support dedicated bearers, which correspond to QCI values 1 through 4. [Table 56 on page 503](#) shows the supported QoS Class Identifiers and the associated set of QoS characteristics, as defined in the 3GPP standards.

**Table 56: QoS Class Identifiers for 4G Networks**

| Qos Class Identifier | Priority | Packet Delay (in milliseconds) | Packet Error Loss Rate | Example Services                                                            |
|----------------------|----------|--------------------------------|------------------------|-----------------------------------------------------------------------------|
| 5                    | 1        | 100 ms                         | $10^{-6}$              | IP Multimedia Subsystem (IMS) signaling                                     |
| 6                    | 7        | 10 ms                          | $10^{-3}$              | Voice, video (live streaming), Interactive gaming                           |
| 7                    | 6        | 300 ms                         | $10^{-6}$              | Video (buffered streaming), TCP-based (e-mail, chat, FTP, P2P file sharing) |
| 8                    | 8        |                                |                        |                                                                             |
| 9                    | 9        |                                |                        |                                                                             |

The priority associated with each QCI is applied when packets are forwarded across the network. Higher-priority packets are transferred before lower-priority packets.

The packet delay budget associated with each QCI defines an upper boundary for the packet delay between the user equipment and the policy and charging enforcement function (PCEF) within the broadband gateway.

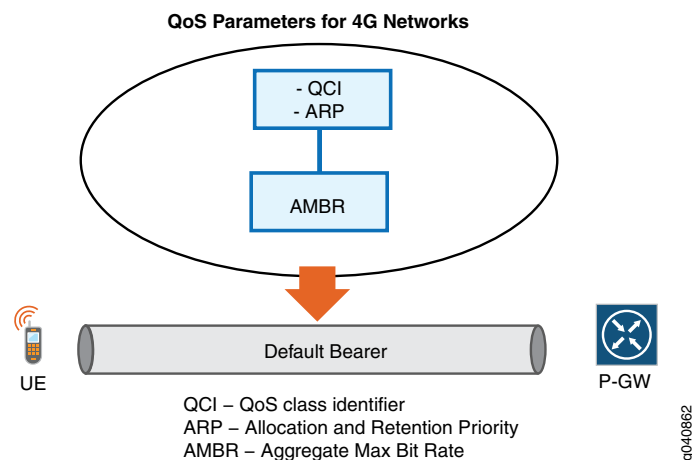
The packet error loss rate defines the percentage of higher layer packets—for example, IP packets—that are lost during periods when the network is not congested.



**NOTE:** To define the packet-forwarding treatment for bearer requests received on the broadband gateway, each QCI must be mapped to a forwarding class and packet loss priority (PLP) in the QoS classifier profile. If a QCI is not mapped to a forwarding class and PLP, the classification specified in the bearer request, coming from either the S5 or SGi interface, is carried over.

A policy profile defines the QoS treatment to be applied to default bearer requests based on the configured QoS parameters. [Figure 58 on page 504](#) shows the QoS parameters that the broadband gateway processes to determine whether to limit, upgrade, or reject bearer requests.

Figure 58: Key QoS Parameters for 4G Default Bearer Requests



Each default bearer is associated with a QCI value, aggregate maximum bit rate (AMBR), and allocation and retention priority (ARP) value.

### Aggregate Maximum Bit Rate

The aggregate maximum bit rate (AMBR) defines the maximum allowed throughput for user equipment (UE) based on the sum of all total bit rates that all non-GBR bearers associated with an access point name (APN) are allowed to use. Thus the AMBR limits the total non-GBR traffic for an APN. You can configure the AMBR independently for uplink and downlink traffic.

### Allocation and Retention Priority

The allocation and retention priority (ARP) indicates a priority level for the allocation and retention of bearers. The mobile network uses ARP to decide whether to accept a request to establish a bearer, or reject the request when resources are limited. When performing admission control and network resources are limited, the network uses the ARP to prioritize establishing or modifying bearers with a higher ARP (lower numerically) over bearers with a lower ARP. The more sensitive the QoS application, the lower the corresponding PL or ARP value.

In a 4G network, ARP priority level (PL) values range from 1 through 15, where 1 corresponds to the highest priority and 15 corresponds to the lowest priority. In a 3G network, GTPv1 (pre-Release 9) ARP values range from 1 through 3, where 1 corresponds to the highest priority and 3 corresponds to the lowest priority. By default, the broadband gateway converts GTPv1 pre-Release 9 ARP values to Release 9 ARP values, based on the 3GPP specification 23.401 ANNEX E. [Table 57 on page 504](#) shows how the broadband gateway maps GTPv1 pre-Release 9 bearer parameter ARP values to Release 9 GTPv2 ARP values.

Table 57: Conversion of GTPv1 Pre-Release 9 ARP Values to Release 9 ARP Values

| GTPv1 Pre-release 9 ARP | GTPv1/v2 Release 9 ARP |
|-------------------------|------------------------|
| 1                       | 1                      |
| 2                       | 6                      |

Table 57: Conversion of GTPv1 Pre-Release 9 ARP Values to Release 9 ARP Values (*continued*)

|   |    |
|---|----|
| 3 | 11 |
|---|----|

Conversely, when subscriber calls come in with a pre-Release 9 ARP value, the broadband gateway performs the required ARP conversion to ensure that the call goes back out with the appropriate ARP value. [Table 58 on page 505](#) shows how the broadband gateway converts GTPv2 Release 9 bearer parameter ARP values to GTPv1 pre-Release 9 ARP values.

Table 58: Mapping of Release 9 ARP Values to Pre-Release 9 ARP Values

| GTPv2 Release 9 ARP | GTPv1 Pre-Release 9 ARP |
|---------------------|-------------------------|
| 1-5                 | 1                       |
| 6-10                | 2                       |
| 11-15               | 3                       |

Preemption

The broadband gateway uses ARP values to manage the allocation and retention of resources for bearers. When preemption is enabled, the broadband gateway evaluates the priority level (PL) and the preemption vulnerability (PVI) and preemption capability (PCI) flags in the GTPv2 information element (IE) to determine whether a bearer is a candidate for deletion:

- PCI—Preemption capability information determines whether a bearer with a lower PL priority level should be dropped to free up the required resources.
- PVI—Preemption vulnerability information determines whether a bearer is a candidate for dropping by another preemption capable bearer with a higher PL value.
- PL—Priority level information defines the allocation and retention priority of the bearer.



**NOTE:** For GTPv1 pre-Release9 PDP contexts, the broadband gateway uses ARP values to determine the preemption capability and preemption vulnerability. By default, preemption capability and preemption vulnerability are enabled. Optionally, you can configure the `gtpv1-pci-disable` and `gtpv1-pvi-disable` options to disable preemption capability and/or preemption vulnerability.

Related Documentation

- [Call Admission Control Overview on page 506](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 508](#)
- [Applying Rewrite Rules on Mobile Interfaces Overview on page 510](#)
- [Configuring QoS on the Broadband Gateway Overview on page 516](#)
- [Configuring S-GW-Specific CAC Parameters on page 581](#)

- [Example: Configuring QoS and CAC on a S-GW on page 582](#)

## Call Admission Control Overview

---

Call admission control (CAC) on the MobileNext Broadband Gateway ensures that required network resources are available for real-time data traffic such as voice and video. CAC maintains information about all resources available on the broadband gateway and resources that have been allocated to bearers. Call admission is based on resource availability and the priority of the bearer, and allows the broadband gateway to reject or downgrade (Create or Modify) bearer requests when the CPU, memory, or bearer load for upstream or downstream traffic exceeds configured CAC thresholds.

This topic covers:

- [Enforcing Call Admission Control on page 506](#)
- [Managing Bandwidth on page 506](#)
- [Managing the Number of Bearers on page 507](#)
- [Managing Resource Thresholds on page 507](#)
- [Default Resource Threshold Settings on page 507](#)

## Enforcing Call Admission Control

Call admission control is enforced only when a local policy profile is configured at the system level or access point name (APN) level on the broadband gateway.

## Managing Bandwidth

A bandwidth pool limits the number of guaranteed bit rate (GBR) bearers that can be supported on the broadband gateway (at the APN level or system level) per traffic class. Because a broadband gateway provides a limited amount of bandwidth, it must keep track of the amount of allocated bandwidth when receiving create/update PDP context requests with GBR requirements.



**NOTE:** You configure bandwidth pools to provide GBR requirements for 3G networks.

---

When admitting bearers, and especially bearers with GBR requirements, the broadband gateway must reject requests when the bandwidth requirements cannot be guaranteed. However, the bandwidth guarantees are only soft guarantees in that the broadband gateway can only restrict the total bandwidth guaranteed to the bearers; no hardware resources are allocated in the system for a bearer with a GBR.

Bandwidth is reserved at the system level or access point name (APN) level based on where the local policy is configured. A local policy configured at the system level specifies a bandwidth pool for all APNs that do not have an explicitly configured bandwidth pool. A bandwidth pool associated with multiple APNs is shared among all bearers of those



APNs. A local policy configured at the APN level specifies a bandwidth pool reserved for bearers associated with the specific APN.

## Managing the Number of Bearers

A broadband gateway provides resource control for the number of bearers. In the control plane and data plane, a set of resources is allocated to each bearer regardless of the bandwidth requirements for the bearer, and the broadband gateway should always specify the maximum number of bearers allowed at the system level, or APN level, or both. When the number of bearers at the system level or APN level reaches the maximum limit, no bearer requests other than delete bearer requests are allowed.

## Managing Resource Thresholds

You configure the following parameters for resource thresholds to control traffic flow at either the system level or APN level:

- Bearer load—Specifies a more precise level of admission control when bearer load reaches a configured lower or upper threshold.
- Memory load—Specifies a more precise level of admission control when memory utilization reaches a configured lower or upper threshold.
- CPU load—Specifies a more precise level of admission control when CPU load reaches a configured lower or upper threshold.

Each threshold parameter includes a low and high threshold setting that is associated with an allocation and retention priority (ARP).



**NOTE:** When subscriber traffic on the broadband gateway exceeds the configured low or high resource threshold settings, only Create Session requests with a higher-priority ARP (GTPv1) or PL (GTPv2) are allowed. When the limits for bearer, CPU, or memory load exceed the configured threshold limits, the broadband gateway can preempt bearers with a lower priority.

## Default Resource Threshold Settings

If you do not explicitly configure resource threshold settings on the broadband gateway, the following resource threshold default values apply:

- CPU and bearer load default values:
  - High threshold—85 percent
  - High threshold priority level—5
  - Low threshold—70 percent
  - Low threshold priority level—10

- Memory load default values:
  - High threshold—90 percent
  - High threshold priority level—5
  - Low threshold—80 percent
  - Low threshold priority level—10

**Related Documentation**

- [Quality of Service Overview on page 499](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 508](#)
- [Policing Subscriber Traffic on the Broadband Gateway Overview on page 509](#)
- [Configuring QoS on the Broadband Gateway Overview on page 516](#)
- [Configuring S-GW-Specific CAC Parameters on page 581](#)
- [Example: Configuring QoS and CAC on a S-GW on page 582](#)

---

## Class of Service (CoS) Policy Profile Overview

---

You configure a CoS policy profile to define additional call admission control characteristics that the MobileNext Broadband Gateway uses during call setup to decide whether to admit a bearer.

A CoS policy profile manages the following resources and settings:

- Maximum QoS Class Identifier (QCI)—Any default bearer set up with a QCI value that is of a higher priority (numerically lower) than the configured maximum QCI value is downgraded by default. A Modify bearer request that specifies a higher-priority QCI than the configured maximum QCI will be downgraded to a maximum QCI value. Optionally, you can configure the broadband gateway to allow bearers with a lower-priority QCI than the configured value to be upgraded or rejected.
- Maximum (non-GBR) traffic class—Any bearer set up with a traffic class or traffic handling priority that is of a higher traffic class than the configured maximum traffic class (mapped to a QCI value 5 through 9) is downgraded by default. A modify bearer request that is of a higher traffic class than the configured maximum traffic class is downgraded to the maximum traffic class. Optionally, you can configure the broadband gateway to allow bearer requests of a lower traffic class to be upgraded or rejected.
- Aggregate maximum bit rate (AMBR)—In a 4G network, the AMBR specifies the total maximum bit rate for all default bearers associated with a specific gateway or access point name (APN). A bearer request that specifies a higher AMBR than the configured value is downgraded by default. Optionally, you can configure the broadband gateway to allow bearers with a higher AMBR than the configured value to be upgraded or rejected. You can configure different AMBR values for uplink and downlink traffic.
- Maximum bit rate (MBR)—In a 3G network, each traffic class specifies the maximum bit rate allowed. A bearer request that specifies a higher MBR than the configured maximum value is downgraded by default. Optionally, you can configure the broadband

gateway to allow bearers with a lower MBR than the configured value to be upgraded or rejected. You can configure different maximum bit rates for uplink and downlink traffic.

- **Guaranteed bit rate (GBR)**— In a 3G network, the conversational and streaming traffic classes specify the maximum guaranteed bit rate allowed. A bearer request that specifies a higher GBR than the configured maximum value is downgraded by default. Optionally, you can configure the broadband gateway to allow bearers with a lower GBR than the configured value to be upgraded or rejected. You can configure different guaranteed bit rates for uplink and downlink traffic.

#### Related Documentation

- [Quality of Service Overview on page 499](#)
- [Call Admission Control Overview on page 506](#)
- [Configuring QoS on the Broadband Gateway Overview on page 516](#)
- [Configuring S-GW-Specific CAC Parameters on page 581](#)
- [Example: Configuring QoS and CAC on a S-GW on page 582](#)

## Policing Subscriber Traffic on the Broadband Gateway Overview

To enforce bandwidth limits for subscriber traffic on the MobileNext Broadband Gateway, you configure the policer action to apply to traffic that exceeds the maximum or guaranteed bit rates. The policer actions control packet behavior by transmitting or changing the packet loss priority (PLP) of packets when the subscriber traffic exceeds configured limits.

The broadband gateway uses a two-rate policer to enforce bandwidth rates.

For non-GBR bearers, you configure the **violate-action** option to specify how bearer data is treated when it exceeds the maximum bit rate (MBR) value with which a PDP context was established or the aggregate maximum bit rate (AMBR) value with which a default bearer was established. For GBR bearers, you configure the **violate-action** option to specify how bearer data is treated traffic exceeds the configured MBR and the **exceed-action** option to define how guaranteed bit rate (GBR) bearer data is treated when the GBR exceeds the GBR value with which the PDP context was established.

For non-GBR bearers, **violate-action** option allows either of the following actions for bearers that exceed the AMBR (4G) or MBR (3G):

- Transmit the packet without changing the PLP
- Set the PLP to “high.”



**NOTE:** The default behavior of **violate-action** is drop. Data that exceeds the MBR is dropped by default. Data within the MBR is transmitted with PLP set to “high.”

For GBR bearers (3G subscribers), the broadband gateway supports the following options:

- **exceed-action**—Specifies one of the following actions for bearers that exceed the GBR:
  - Set the PLP to “high” (the default).
  - Transmit the packet without changing the PLP.
- **violate-action**—Specifies one of the following actions for bearers that exceed the MBR:
  - Set the PLP to “high.”
  - Transmit the packet without changing PLP.



**NOTE:** The default behavior of **exceed-action** is to set the PLP to “high” and **violate-action** is to drop. Data that exceeds the GBR but is within the MBR is transmitted with PLP set to “high”. Data that exceeds the MBR is dropped.

---

**Related  
Documentation**

- [Quality of Service Overview on page 499](#)
- [Call Admission Control Overview on page 506](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 508](#)
- [Configuring QoS on the Broadband Gateway Overview on page 516](#)
- [Configuring S-GW-Specific CAC Parameters on page 581](#)
- [Example: Configuring QoS and CAC on a S-GW on page 582](#)

---

## Applying Rewrite Rules on Mobile Interfaces Overview

---

For each mobile interface on the MobileNext Broadband Gateway (one mobile interface per access point name [APN]), you must configure ingress and egress rewrite rules and apply them to the interfaces. This provides the required DSCP marking for subscriber packets. The rewrite rules that you configure and apply to a mobile interface provides the required DSCP marking for all subscriber packets associated with the APN to which the mobile interface maps.

An ingress rewrite rule (**ingress-rewrite-rules**) sets the type-of-service (ToS) bits based on the forwarding class and loss priority of the upstream subscriber packet received on the mobile interface. For upstream traffic, the rewrite rule is applied to packets exiting the anchor Packet Forwarding Engine towards the Gi or SGi interface. The ingress rewrite rule writes into the outer IP header only.

An egress rewrite rule (**rewrite-rules**) sets the ToS bits based on the forwarding class and loss priority of an downstream subscriber packet received on the mobile interface. For downstream subscriber traffic, the rewrite rule is applied to packets exiting the (egress) anchor Packet Forwarding Engine towards the Gn or S5 interface. An egress rewrite rule writes into the outer IP header, and optionally, inner IP header for the GPRS tunneling protocol (GTP) packet.



**NOTE:** Egress rewrite rules must not be applied to the Ethernet interfaces on MX Series routers that receive downstream subscriber traffic from the broadband gateway. If configured, egress rewrite rules on the Ethernet interface will overwrite the QoS treatment configured on the broadband gateway for subscriber packets.

#### Related Documentation

- [Quality of Service Overview on page 499](#)
- [Call Admission Control Overview on page 506](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 508](#)
- [Configuring QoS on the Broadband Gateway Overview on page 516](#)
- [Understanding Upstream and Downstream Processing of ToS Values in GTP-U Packets on page 511](#)
- [Configuring S-GW-Specific CAC Parameters on page 581](#)
- [Example: Configuring QoS and CAC on a S-GW on page 582](#)

## Understanding Upstream and Downstream Processing of ToS Values in GTP-U Packets

To provide the required QoS treatment for upstream and downstream subscriber traffic, GTP-U packets are processed at multiple points in the data path.

This topic describes the upstream and downstream operations performed on GTP-U packets on the MobileNext Broadband Gateway.

- [Processing of ToS Values for Upstream Subscriber Packets on page 511](#)
- [Processing of ToS Values for Downstream Subscriber Packets on page 512](#)

### Processing of ToS Values for Upstream Subscriber Packets

The broadband gateway processes upstream GTP-U packets from a Gn/S5 interface to a Gi/SGi interface.

The following steps describe the processing of type-of-service (ToS) values for upstream GTP-U packets:

1. A GTP-U packet arrives on the mobile (Ethernet) interface, and a behavior aggregate (BA) classifier evaluates the ToS value of the subscriber packet to derive an appropriate Junos OS forwarding class and packet loss priority (PLP).
2. The GTP-U packet is sent to the appropriate queue on the Packet Forwarding Engine. (The forwarding class determines the queue.)
3. The packet is sent to the anchor Packet Forwarding Engine where the GTP packet header is decapsulated.



**NOTE:** A classifier profile must be configured on the broadband gateway to provide a mapping from a traffic class/QCI to a forwarding class and PLP.

4. Subscriber tunnel endpoint identifier (TEID) lookup identifies the traffic class or QCI for the packet. The traffic class or QCI is mapped to a forwarding class and PLP, based on the classifier profile configured on the broadband gateway.
5. The packet is sent out on the anchor Packet Forwarding Engine where the ingress rewrite rule applied on the mobile interface takes the forwarding class and PLP (Step 4) as input values to derive the appropriate DSCP marking before sending the packet to the SGi/Gi interface.



**NOTE:** An ingress rewrite rule must be configured and applied to each mobile interface to provide the required DSCP marking for upstream subscriber traffic.

6. The packet is sent out on the correct Gi or SGi interface.

## Processing of ToS Values for Downstream Subscriber Packets

The broadband gateway processes downstream GTP-U packets from a Gi or SGi to a Gn or S5 interface.

The following steps describe the processing of ToS values for downstream GTP-U packets:

1. The GTP-U packet arrives from the Gi or SGi interface, and is sent to the anchor Packet Forwarding Engine associated with the virtual routing and forwarding (VRF) route.
2. On the anchor Packet Forwarding Engine, an IP address lookup identifies the TEID for the GTP header and, before encapsulation, the traffic class/QCI maps to a forwarding class and PLP, based on the classifier profile configured on the broadband gateway.
3. The packet is sent out from the anchor Packet Forwarding Engine where the egress rewrite rule applied on the mobile interface takes the forwarding class and PLP (Step 2) as input values to derive the appropriate DSCP marking.
4. The packet is encapsulated with TEID and outer IP address in the GTP header, which is used for route table lookup for the SGSN/S-GW and sent to the egress Packet Forwarding Engine interface.
5. The packet is sent out on the correct Gn or S5 interface.

### Related Documentation

- [Applying Rewrite Rules on Mobile Interfaces Overview on page 510](#)
- [Configuring S-GW-Specific CAC Parameters on page 581](#)
- [Example: Configuring QoS and CAC on a S-GW on page 582](#)

## Understanding How NQN and Upgrade Flags in PDP Contexts Affect QoS Upgrade Behavior

GTPv1 subscriber packets that contain NQN and Upgrade flags in Create/Update PDP context requests can affect the QoS treatment during processing on the MobileNext Broadband Gateway. Consequently, incoming requests might not be upgraded even though the local policy configured on the broadband gateway warrants an upgrade of the traffic class, maximum bit rate, or ARP for subscriber packets.

Figure 59 on page 513 shows how negotiated QoS values are affected based on the presence of NQN or Upgrade flags in Create/Update PDP context requests.

**Figure 59: QoS Negotiation Behavior for PDP Contexts with NQN and Upgrade Flags**

| Case              | GTP Message | Upgrade Flag | NQN | Local Policy   | Requested QoS | Response | Local Policy | Requested QoS  | Response    | Local Policy  | Requested QoS | Response |
|-------------------|-------------|--------------|-----|----------------|---------------|----------|--------------|----------------|-------------|---------------|---------------|----------|
| 0- False, 1- True |             |              |     |                |               |          |              |                |             |               |               |          |
| 1                 | Create      | 0            | 0   | 1024-Upgrade   | 512           | 512      | TC-Upgrade   | interactive    | interactive | ARP-Upgrade   | 2             | 2        |
| 2                 | Create      | 0            | 0   | 1024-Upgrade   | 1500          | 1024     | TC-Upgrade   | conv           | streaming   | ARP-Upgrade   | 1             | 2        |
| 3                 | Create      | 1            | 0   | 1024-Upgrade   | 512           | 1024     | TC-Upgrade   | interactive    | streaming   | ARP-Upgrade   | 3             | 2        |
| 4                 | Create      | 1            | 0   | 1024-Upgrade   | 1500          | 1024     | TC-Upgrade   | conv           | streaming   | ARP-Upgrade   | 1             | 2        |
| 5                 | Create      | 0            | 0   | 1024-Downgrade | 512           | 512      | TC-Downgrade | interactive    | interactive | ARP-Downgrade | 3             | 3        |
| 6                 | Create      | 0            | 0   | 1024-Downgrade | 1500          | 1024     | TC-Downgrade | conv           | streaming   | ARP-Downgrade | 1             | 2        |
| 7                 | Create      | 1            | 0   | 1024-Downgrade | 512           | 512      | TC-Downgrade | interactive    | interactive | ARP-Downgrade | 3             | 3        |
| 8                 | Create      | 1            | 0   | 1024-Downgrade | 1500          | 1024     | TC-Downgrade | conv           | streaming   | ARP-Downgrade | 1             | 2        |
| 9                 | Update      | 0            | 0   | 1024-Upgrade   | 512           | 512      | TC-Upgrade   | interactive    | interactive | ARP-Upgrade   | 3             | 3        |
| 10                | Update      | 0            | 0   | 1024-Upgrade   | 1500          | 1024     | TC-Upgrade   | conversational | streaming   | ARP-Upgrade   | 1             | 2        |
| 11                | Update      | 1            | 0   | 1024-Upgrade   | 512           | 512      | TC-Upgrade   | interactive    | interactive | ARP-Upgrade   | 3             | 3        |
| 12                | Update      | 1            | 0   | 1024-Upgrade   | 1500          | 1024     | TC-Upgrade   | conversational | streaming   | ARP-Upgrade   | 1             | 2        |
| 13                | Update      | 0            | 1   | 1024-Upgrade   | 512           | 512      | TC-Upgrade   | interactive    | interactive | ARP-Upgrade   | 3             | 3        |
| 14                | Update      | 0            | 1   | 1024-Upgrade   | 1500          | REJECT   | TC-Upgrade   | conversational | reject      | ARP-Upgrade   | 1             | reject   |
| 15                | Update      | 1            | 1   | 1024-Upgrade   | 512           | 512      | TC-Upgrade   | interactive    | interactive | ARP-Upgrade   | 3             | 3        |
| 16                | Update      | 1            | 1   | 1024-Upgrade   | 1500          | REJECT   | TC-Upgrade   | conversational | reject      | ARP-Upgrade   | 1             | reject   |
| 17                | Update      | 0            | 0   | 1024-Downgrade | 512           | 512      | TC-Downgrade | interactive    | interactive | ARP-Downgrade | 3             | 3        |
| 18                | Update      | 0            | 0   | 1024-Downgrade | 1500          | 1024     | TC-Downgrade | conversational | streaming   | ARP-Downgrade | 1             | 2        |
| 19                | Update      | 1            | 0   | 1024-Downgrade | 512           | 512      | TC-Downgrade | interactive    | interactive | ARP-Downgrade | 3             | 3        |
| 20                | Update      | 1            | 0   | 1024-Downgrade | 1500          | 1024     | TC-Downgrade | conversational | streaming   | ARP-Downgrade | 1             | 2        |
| 21                | Update      | 0            | 1   | 1024-Downgrade | 512           | 512      | TC-Downgrade | interactive    | interactive | ARP-Downgrade | 3             | 3        |
| 22                | Update      | 0            | 1   | 1024-Downgrade | 1500          | REJECT   | TC-Downgrade | conversational | reject      | ARP-Downgrade | 1             | reject   |
| 23                | Update      | 1            | 1   | 1024-Downgrade | 512           | 512      | TC-Downgrade | interactive    | interactive | ARP-Downgrade | 3             | 3        |
| 24                | Update      | 1            | 1   | 1024-Downgrade | 1500          | REJECT   | TC-Downgrade | conversational | reject      | ARP-Downgrade | 1             | reject   |

For Create PDP context requests arriving on the broadband gateway, the NQN and Upgrade flags can affect QoS negotiation as follows:

The Upgrade flag in a Create PDP context affects the upgrade behavior configured in the local policy for MBR, GBR, traffic class, and ARP value.

- For Cases 1 and 3 in Figure 59 on page 513, the QoS response results are different because the Upgrade Flag is set for Case 3. For example, MBR 512 versus 1024, traffic class interactive versus streaming, and ARP upgrade occurs for Case 3 only.
- For Cases 9 and 11 in Figure 59 on page 513, the combination of NQN and Upgrade flags in the Update PDP context prevent the expected upgrade of requested QoS values for MBR, traffic class, and ARP behavior, as configured in the local policy.



**NOTE:** The Upgrade flag in a Create PDP context does not affect the downgrade behavior configured in the local policy.

For Update PDP context requests arriving on the broadband gateway, the NQN and Upgrade flags can also affect QoS negotiation. For example, for Cases 14 and 16 in [Figure 59 on page 513](#), the request is rejected because the NQN flag is set.



**NOTE:** The Upgrade flag in a Update PDP context does not affect the downgrade behavior configured in the local policy.

---

**Related  
Documentation**

- [Class of Service \(CoS\) Policy Profile Overview on page 508](#)
- [Configuring S-GW-Specific CAC Parameters on page 581](#)
- [Example: Configuring QoS and CAC on a S-GW on page 582](#)



## CHAPTER 22

# Configuring Quality of Service

- [Configuring QoS on the Broadband Gateway Overview on page 516](#)
- [Configuring the Maximum Number of Bearers on page 517](#)
- [Configuring Bandwidth Pools on page 518](#)
- [Configuring Preemption for Call Admission Control on page 519](#)
- [Configuring Resource Thresholds for 3G and 4G Networks on page 520](#)
- [Configuring a Classifier Profile for 3G and 4G Networks on page 521](#)
- [Configuring a CoS Policy Profile for 4G Networks on page 523](#)
- [Configuring a CoS Policy Profile for 3G Networks on page 526](#)
- [Configuring a CoS Policy Profile for 3G and 4G Networks on page 531](#)
- [Configuring a Local Policy on page 537](#)
- [Applying a Local Policy on page 538](#)
- [Configuring Ingress Rewrite Rules for a Mobile Interface on page 539](#)
- [Configuring Egress Rewrite Rules for a Mobile Interface on page 539](#)
- [Applying Ingress Rewrite Rules to a Mobile Interface on page 540](#)
- [Applying Egress Rewrite Rules to Mobile Interfaces on page 541](#)
- [Example: Configuring Quality of Service on GGSN/P-GW on page 542](#)
- [Verifying Quality of Service on page 579](#)
- [Configuring S-GW-Specific CAC Parameters on page 581](#)
- [Example: Configuring QoS and CAC on a S-GW on page 582](#)

## Configuring QoS on the Broadband Gateway Overview

---

Configuring quality of service (QoS) on the MobileNext Broadband Gateway for a 3G or 4G network is a multistep process in which you configure the resource threshold profiles, classifier profiles, and CoS policy profiles that are then specified in local policies to provide call admission control (CAC) and prioritization of subscriber traffic when the network load increases.

The following steps describe the high-level process for configuring QoS for 3G and 4G networks:

1. Configure the number of bearers at the system level or access point name (APN) level.
2. Configure bandwidth pools to ensure that sufficient bandwidth is available when guaranteed bit rate (GBR) packet data protocol (PDP) contexts are created or modified. Call admission control (CAC) uses bandwidth pools to either accept or reject the GBR PDP contexts based on availability of bandwidth, or to negotiate and reserve the bandwidth.
3. Configure preemption at the gateway level to enable preemption for GTPv2 bearers. For GTPv1 pre-Release 9 PDP contexts, you can enable preemption capability and preemption vulnerability independently. The broadband gateway uses ARP values to manage the allocation and retention of resources for bearers. When preemption is enabled, the broadband gateway evaluates the priority level (PL) and the preemption vulnerability (PVI) and preemption capability (PCI) flags in the GTPv2 information element (IE) to determine whether a bearer is a candidate for deletion.



**NOTE:** Preemption is disabled by default.

4. Configure a resource threshold profile to define call admission control to manage load thresholds for the number of bearers, memory load, and CPU load.
5. Configure a classifier profile—Each traffic class or traffic handling priority (3G) and QoS Class Identifier (QCI) (4G) is mapped to a forwarding class and packet loss priority (PLP).



**NOTE:** For 3G bearers, the broadband gateway converts the traffic class to a QCI based on the 3GPP specification 23.401 ANNEX E. Thus, to configure packet forwarding for 3G traffic classes, you map the forwarding class and PLP for the QCI that maps to a traffic class. For more information about how 3G traffic classes are mapped to QCI values, see [“Quality of Service Overview” on page 499](#).



**NOTE:** You can configure separate classifier profiles for home, roaming, and visitor subscriber traffic.

6. Configure a class-of-service (CoS) policy profile to define how traffic is divided into classes and specify whether to upgrade or limit bearer requests based on availability of system resources.



**NOTE:** You can configure separate CoS policy profiles for home, roaming, and visitor subscriber traffic.

7. Configure a local policy to define overall QoS treatment for subscriber traffic in 3G networks or 4G networks. A local policy includes the configuration of bandwidth pools (for uplink and downlink), classifier profiles, a resource threshold profile, and CoS policy profiles. You can configure separate CoS policy profiles for home, roaming, and visitor subscriber traffic.



**NOTE:** You can configure multiple classifier profiles and CoS policy profiles to address QoS configuration requirements for home, roaming, and visitor subscriber traffic.

8. Apply a local policy at the gateway level or APN level.
9. Configure ingress and egress rewrite rules for upstream and downstream subscriber traffic.
10. Apply ingress and egress rewrite rules on mobile interfaces to provide Differentiated Services code point (DSCP) marking for upstream and downstream subscriber traffic.

#### Related Documentation

- [Call Admission Control Overview on page 506](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 508](#)
- [Policing Subscriber Traffic on the Broadband Gateway Overview on page 509](#)
- [Applying Rewrite Rules on Mobile Interfaces Overview on page 510](#)
- [Configuring S-GW-Specific CAC Parameters on page 581](#)
- [Example: Configuring QoS and CAC on a S-GW on page 582](#)

## Configuring the Maximum Number of Bearers

You configure the maximum bearers to specify an upper limit on the number of bearers allowed at the system level or access point name (APN) level.

When the total number of active bearers at the gateway level or APN level reaches the maximum configured limit, the MobileNext Broadband Gateway rejects new bearer requests.

- Configure the maximum number of active bearers allowed at the gateway level.

```
[edit unified-edge gateways ggsn-pgw MBG1]
user@host# set maximum-bearers 5000000
```

- For each APN, configure the maximum number of active bearers allowed at the APN level.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1]  
user@host# set maximum-bearers 10000
```

**Related  
Documentation**

- [Configuring QoS on the Broadband Gateway Overview on page 516](#)
- [Call Admission Control Overview on page 506](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 508](#)
- [Configuring S-GW-Specific CAC Parameters on page 581](#)
- [Example: Configuring QoS and CAC on a S-GW on page 582](#)

---

## Configuring Bandwidth Pools

You configure a bandwidth pool to ensure that sufficient bandwidth is available when guaranteed bit rate (GBR) packet data protocol (PDP) contexts are created or modified. Call admission control (CAC) uses bandwidth pools to either accept or reject the GBR PDP contexts based on availability of bandwidth, or to negotiate and reserve the bandwidth.

To configure a bandwidth pool:

1. Specify a name for the bandwidth pool.

```
[edit unified-edge cos-cac]  
user@host# edit gbr-bandwidth-pools bw-pool-1
```

2. Configure the total bandwidth of the pool, in megabits per second (Mbps).

```
[edit unified-edge cos-cac gbr-bandwidth-pools bw-pool-1]  
user@host# set maximum-bandwidth 500000
```

3. (Optional) Specify that when the bearer load on the broadband gateway reaches the configured bandwidth threshold, then create or modify PDP context requests can be downgraded, starting with lower priority requests.

```
[edit unified-edge cos-cac gbr-bandwidth-pools bw-pool-1]  
user@host# set downgrade-gtp-v1-gbr-bearers
```



**NOTE:** If the `downgrade-gtp-v1-gbr-bearers` option is configured and the bandwidth threshold is reached, create or modify PDP context requests arriving on the broadband gateway are downgraded to the Background traffic class. If the `downgrade-gtp-v1-gbr-bearers` option is not configured and the bandwidth threshold is reached, create or modify PDP context requests arriving on the broadband gateway are rejected.

---

**Related  
Documentation**

- [Configuring QoS on the Broadband Gateway Overview on page 516](#)

## Configuring Preemption for Call Admission Control

You can enable preemption at the gateway level to enable the preemption capability indicator (PCI) and preemption vulnerability indicator (PVI) flags. Preemption is disabled by default. In a 4G network, the PVI and PCI bit values are included with the allocation and retention priority (ARP). In a 3G network, PDP context requests do not support the PVI and PCI flags, and the MobileNext Broadband Gateway uses ARP values to determine preemption capability and preemption vulnerability. GTPv1 subscribers. Preemption takes effect when the high threshold for bearer or memory load (configured in a **resource-threshold-profile**) is reached on the MobileNext Broadband Gateway.

To enable preemption on the broadband gateway:

- To enable preemption for both GTPv1 and GTPv2 subscribers:

```
[edit unified-edge gateways ggsn-pgw MBG1 preemption]
user@host# set enable
```

- To enable only PVI for GTPv1 subscribers:

```
[edit unified-edge gateways ggsn-pgw MBG1 preemption]
user@host# set enable
user@host# set gtpv1-pci-disable
```

- To enable only PCI for GTPv1 subscribers:

```
[edit unified-edge gateways ggsn-pgw MBG1 preemption]
user@host# set enable
user@host# set gtpv1-pvi-disable
```

### Related Documentation

- [Configuring QoS on the Broadband Gateway Overview on page 516](#)
- [Call Admission Control Overview on page 506](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 508](#)
- [Configuring S-GW-Specific CAC Parameters on page 581](#)
- [Example: Configuring QoS and CAC on a S-GW on page 582](#)

## Configuring Resource Thresholds for 3G and 4G Networks

You configure a resource threshold profile to ensure that when the bearer load, CPU load, or memory load at the access point name (APN) or gateway level on the MobileNext Broadband Gateway reaches a specified threshold, only create session requests that meet or exceed a designated allocation and retention priority (ARP) level are admitted.

Table 59 on page 520 shows the mapping of EPS bearer ARP to Release 99 bearer parameter ARP.

**Table 59: Mapping of EPS Bearer ARP to Release 99 Bearer Parameter ARP**

| EPS Bearer Priority Level | Release 99 Bearer Parameter ARP |
|---------------------------|---------------------------------|
| 1                         | 1                               |
| 6                         | 2                               |
| 11                        | 3                               |

To configure a resource threshold profile:

1. Specify a name for the resource threshold.

```
[edit unified-edge cos-cac]
user@host# edit resource-threshold-profiles resource-threshold-1
```

2. Configure the bearer priority level and threshold limits for the number of bearers:

- a. Configure the bearer priority when the number of bearers reaches the lower threshold. The following configuration specifies that when the number of bearers exceeds 70 percent of the allowed limit, only Create Session requests with a priority level equal to or higher than the specified ARP value are accepted:

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1
bearers-load low]
user@host# set percentage 70
user@host# priority-level 10
```

- b. Configure the bearer priority when the number of bearers reaches the upper threshold. The following configuration specifies that when the number of bearers exceeds 85 percent, only Create Session requests with a priority level equal to or higher than the specified ARP values are accepted:

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1
bearers-load high]
user@host# set percentage 85
user@host# set priority-level 4
```

3. Configure the bearer priority and threshold limits for the CPU load:

- a. Configure a lower limit for the CPU load.

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1 cpu
low]
```

```
user@host# set percentage 70
user@host# set priority-level 10
```

- b. Configure an upper limit for the CPU load.

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1 cpu
high]
user@host# set percentage 85
user@host# set priority-level 4
```

4. Configure the bearer priority and threshold limits for the memory load:

- a. Configure a lower limit for the memory load.

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1 memory
low]
user@host# set percentage 70
user@host# set priority-level 10
```

- b. Configure an upper limit for the memory load.

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1 memory
high]
user@host# set percentage 85
user@host# set priority-level 10
```

#### Related Documentation

- [Configuring QoS on the Broadband Gateway Overview on page 516](#)
- [Call Admission Control Overview on page 506](#)
- [Example: Configuring Quality of Service on GGSN/P-GW on page 542](#)
- [Configuring S-GW-Specific CAC Parameters on page 581](#)
- [Example: Configuring QoS and CAC on a S-GW on page 582](#)

## Configuring a Classifier Profile for 3G and 4G Networks

A classifier profile defines the quality of service (QoS) classification for a MobileNext Broadband Gateway configured as a Gateway GPRS Support Node/Packet Data Network Gateway (GGSN/P-GW). You can configure a QoS class identifier (QCI) value and associated forwarding class and loss priority to define the packet-forwarding treatment for both 3G and 4G bearers. Each QCI is associated with priority, delay, and packet loss values.



**NOTE:** The broadband gateway maps Release 99 QoS parameter values to standardized QCI values as defined in GTTP Specification 23.401 ANNEX E.

To configure a classifier profile to map each QCI value to a forwarding class and packet loss priority:

1. Specify a name for the classifier profile.

```
[edit unified-edge cos-cac]
```

```
user@host# edit classifier-profiles classifier-profile-1
```

2. Configure a packet-forwarding treatment that maps to the conversational traffic class.

```
[edit unified-edge cos-cac classifier-profiles classifier-profile-1]  
user@host# set qos-class-identifier 2 forwarding-class af3 loss-priority low
```

3. Configure a packet-forwarding treatment that maps to the streaming traffic class.

```
[edit unified-edge cos-cac classifier-profiles classifier-profile-1]  
user@host# set qos-class-identifier 4 forwarding-class af2 loss-priority low
```

4. Configure a packet-forwarding treatment for IP Multimedia Subsystem (IMS) signaling traffic that also maps to the Interactive traffic class with Traffic Handling Priority (THP) 1.

```
[edit unified-edge cos-cac classifier-profiles classifier-profile-1]  
user@host# set qos-class-identifier 5 forwarding-class af2 loss-priority low
```

5. Configure a packet forwarding treatment for video (buffered streaming) traffic that also maps to the Interactive traffic class with THP 2.

```
[edit unified-edge cos-cac classifier-profiles classifier-profile-1]  
user@host# set qos-class-identifier 6 forwarding-class af2 loss-priority low
```

6. Configure a packet forwarding treatment for voice, video (live streaming), and interactive gaming traffic that also maps to the Interactive traffic class with THP 2.

```
[edit unified-edge cos-cac classifier-profiles classifier-profile-1]  
user@host# set qos-class-identifier 7 forwarding-class af3 loss-priority low
```

7. Configure a packet forwarding treatment for background traffic that also maps to the Interactive traffic class with THP 3.

```
[edit unified-edge cos-cac classifier-profiles classifier-profile-1]  
user@host# set qos-class-identifier 8 forwarding-class be loss-priority low
```

#### Related Documentation

- [Configuring QoS on the Broadband Gateway Overview on page 516](#)
- [Example: Configuring Quality of Service on GGSN/P-GW on page 542](#)
- [Configuring S-GW-Specific CAC Parameters on page 581](#)
- [Example: Configuring QoS and CAC on a S-GW on page 582](#)



## Configuring a CoS Policy Profile for 4G Networks

---

In a 4G network, a class-of-service (CoS) policy profile defines the highest QoS Class Identifier (QCI) value that can be accepted at the access point name (APN) level or gateway level, the aggregate maximum bit rate (AMBR) for default bearers, and the allocation and retention priority (ARP). By default, when a bearer request has a higher AMBR value than the value configured in the CoS policy profile, the AMBR value of the bearer request is downgraded. A CoS policy profile also specifies the policer action to take when subscriber traffic exceeds the policer rates.

Before you begin, complete the following tasks:

- Configure a CoS classifier profile.
- Configure a CoS resource threshold profile.

To configure a CoS policy profile for a 4G network:

1. Specify a name for the CoS policy profile.

```
[edit unified-edge cos-cac]  
user@host# edit cos-policy-profiles policy-profile-2
```

2. Negotiate the QCI value for 4G subscribers by doing one of the following:

- Downgrade the QCI value of create session requests that come in with a higher QCI value (numerically lower) than the configured value:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2]  
user@host# set default-bearer-qci 6
```



**NOTE:** When the default (downgrade) behavior is configured, if a create session request comes in with higher QCI value (numerically lower) than the value configured on the broadband gateway, the QCI value is downgraded to the configured value. If a create session request comes in with a lower QCI value (numerically higher) than the configured QCI, the QCI value is accepted as is.

- Upgrade the QCI value of create session requests that come in with a lower QCI value (numerically higher) than the configured value:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2]  
user@host# set default-bearer-qci 6 upgrade
```



**NOTE:** When the upgrade option is configured, if a create session request comes in with higher QCI value (numerically lower) than the value configured on the broadband gateway, the QCI value is downgraded to the configured value. If a create session request comes in with a lower QCI value (numerically higher) than the configured QCI, the QCI value is upgraded to the configured value.

- Reject the QCI value of create session requests that come in with a higher QCI value (numerically lower) than the configured value:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2]  
user@host# set default-bearer-qci 6 reject
```



**NOTE:** When the reject option is configured, if a create session request comes in with higher QCI value (numerically lower) than the value configured on the broadband gateway, the create session request is rejected. If a create session request comes in with a lower QCI value (numerically higher) than the configured QCI, the QCI value is accepted as is.



**NOTE:** If the QCI value is not specified, the broadband gateway uses the UE/SGW requested or negotiated QCI value.

3. Negotiate the ARP value for 4G subscribers when a bearer is established or modified:

- Specify that bearers that come in with a lower ARP (numerically higher) than the configured value are accepted, and bearers with a higher ARP (numerically lower) are downgraded to the configured value (the default behavior):

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2]
user@host# set allocation-retention-priority 7
```

- Specify that bearers that come in with a lower ARP (numerically higher) than the configured value are accepted, and bearers with a higher ARP (numerically lower) are rejected:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2]
user@host# set allocation-retention-priority 7 reject
```



**NOTE:** If the allocation-retention-priority value is not specified, the broadband gateway uses the UE/SGW requested or negotiated ARP value.

4. Negotiate uplink and downlink AMBR for 4G subscribers by doing one of the following:

- Specify that bearer requests with an AMBR value higher than the configured value are downgraded to the configured AMBR value, and bearer requests with a lower value than the configured AMBR value are accepted (the default behavior):

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 aggregate-qos-control]
user@host# set maximum-bit-rate-uplink 15000
user@host# set maximum-bit-rate-downlink 25000
```

- Specify that bearer requests with a lower AMBR value than the configured value are upgraded to the configured AMBR value, and bearer requests with a higher AMBR value than the configured value are downgraded:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 aggregate-qos-control]
user@host# set maximum-bit-rate-uplink 15000 upgrade
user@host# set maximum-bit-rate-downlink 25000 upgrade
```

- Specify that bearer requests with a higher AMBR value than the configured value are rejected, and bearer requests with a lower AMBR value than the configured value are accepted:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 aggregate-qos-control]
user@host# set maximum-bit-rate-uplink 15000 reject
user@host# set maximum-bit-rate-downlink 25000 reject
```

5. Configure the policer action to define how default bearer data is treated when it exceeds the AMBR value with which the default bearer was established.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 policer-action
non-gbr-bearer]
user@host# set violate-action set-loss-priority-high
```

When **violate-action** is configured with **set-loss-priority-high**, data that exceeds the AMBR is transmitted with PLP high.



**NOTE:** By default, bearers that exceed the AMBR are dropped.

---

**Related  
Documentation**

- [Class of Service \(CoS\) Policy Profile Overview on page 508](#)
- [Configuring QoS on the Broadband Gateway Overview on page 516](#)
- [Configuring a CoS Policy Profile for 3G Networks on page 526](#)
- [Configuring a CoS Policy Profile for 3G and 4G Networks on page 531](#)
- [Example: Configuring Quality of Service on GGSN/P-GW on page 542](#)
- [Configuring S-GW-Specific CAC Parameters on page 581](#)
- [Example: Configuring QoS and CAC on a S-GW on page 582](#)

---

## Configuring a CoS Policy Profile for 3G Networks

---

In a 3G network, the class-of-service (CoS) policy profile defines the highest non-GBR traffic class mapped to a QoS class identifier (QCI) that can be accepted at an access point name (APN) or gateway level, the maximum bit rate (MBR), the guaranteed bit rate (GBR) for each traffic class, and the allocation and retention priority (ARP). A CoS policy profile also specifies the policer action to take when subscriber traffic exceeds the configured GBR, MBR, or both. By default, when a PDP context request has a higher MBR or GBR value than the value configured in the CoS policy profile, the packet data protocol (PDP) context request is downgraded.

Before you begin, complete the following tasks:

- Configure a CoS resource threshold profile.
- Configure CoS bandwidth pools.
- Configure a CoS classifier profile.

To configure a CoS policy profile for a 3G network:

1. Specify a name for the CoS policy profile.

```
[edit unified-edge cos-cac]  
user@host# edit cos-policy-profiles policy-profile-2
```

2. Negotiate the non-GBR traffic class for 3G subscribers by doing one of the following:

- Downgrade the traffic class of create PDP context requests that come in with a higher traffic class than the configured value:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2]
user@host# set default-bearer-qci 6
```



**NOTE:** When default (downgrade) behavior is configured, if a create PDP context request comes in with higher traffic class (mapped to QCI) than the value configured on the broadband gateway, the traffic class is downgraded to the configured value. If a create PDP context request comes in with a lower traffic class (numerically higher QCI) than the configured traffic class, then the traffic class is accepted.

- Upgrade the traffic class of create PDP context requests that come in with a lower traffic class (numerically higher QCI) than the configured value:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2]
user@host# set default-bearer-qci 6 upgrade
```



**NOTE:** when upgrade option is configured, if a create PDP context request comes in with higher traffic class (numerically lower QCI) than the value configured on the broadband gateway, the QCI value is downgraded to the configured value. If a create session request comes in with a lower QCI value (numerically higher) than the configured QCI, then the QCI value is upgraded to the configured value.

- Reject the traffic class of create PDP context requests that come in with a higher traffic class (numerically lower QCI) than the configured value:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2]
user@host# set default-bearer-qci 6 reject
```



**NOTE:** When reject option is configured, if a create PDP context comes in with higher traffic class (numerically lower QCI) than the value configured on the broadband gateway, the create PDP context is rejected. If a create PDP context comes in with a lower traffic class (numerically higher QCI) than the configured QCI, then the traffic class is accepted as is.



**NOTE:** If the QCI/traffic class value is not specified, the broadband gateway uses the UE/SGSN requested or negotiated traffic class value.

3. Negotiate the ARP value for 3G a when a PDP context is established or modified:

- Specify that PDP contexts that come in with a lower ARP (numerically higher) than the configured value are accepted, and PDP contexts with a higher ARP (numerically lower) are downgraded to the configured value (the default behavior):

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2]  
user@host# set allocation-retention-priority 7
```

- Specify that PDP contexts that come in with a lower ARP (numerically higher) than the configured value are accepted, and that PDP contexts with a higher ARP (numerically lower) are rejected:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2]  
user@host# set allocation-retention-priority 7 reject
```



**NOTE:** For GTPv1 subscriber traffic received on the broadband gateway, ARP 1 maps to allocation-retention-priority 1, ARP 2 maps to allocation-retention-priority 6, and ARP 3 maps to allocation-retention-priority 11.



**NOTE:** If the allocation-retention-priority value is not specified, the broadband gateway uses the UE/SGSN requested or negotiated ARP value.

- Negotiate uplink and downlink MBR for 3G non-GBR PDP contexts by doing one of the following:

- Specify that PDP context requests that come in with an MBR value higher than the configured value are downgraded to the configured MBR value, and PDP context requests that come in with a lower value than the configured MBR value are accepted (the default behavior):

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]  
user@host# set maximum-bit-rate-uplink 15000  
user@host# set maximum-bit-rate-downlink 25000
```

- Specify that PDP context requests that come in with a lower MBR value than the configured value are upgraded to the configured MBR value, and PDP context requests that come in with a higher MBR value than the configured value are downgraded:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]  
user@host# set maximum-bit-rate-uplink 15000 upgrade  
user@host# set maximum-bit-rate-downlink 25000 upgrade
```

- Specify that PDP context requests that come in with a higher MBR value than the configured value are rejected, and PDP context requests that come in with a lower MBR value than the configured value are accepted:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]  
user@host# set maximum-bit-rate-uplink 15000 reject
```

```
user@host# set maximum-bit-rate-downlink 25000 reject
```

5. Negotiate the uplink and downlink GBR for 3G GBR bearers by doing one of the following:

- Specify that PDP context requests that come in with a GBR value higher than the configured value are downgraded to the configured GBR value, and PDP context requests that come in with a lower value than the configured GBR value are accepted (the default behavior):

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set guaranteed-bit-rate-uplink 15000
user@host# set guaranteed-bit-rate-downlink 25000
```

- Specify that PDP context requests that come in with a lower GBR value than the configured value are upgraded to the configured GBR value, and PDP context requests that come in with a higher GBR value than the configured value are downgraded:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set guaranteed-bit-rate-uplink 15000 upgrade
user@host# set guaranteed-bit-rate-downlink 25000 upgrade
```

- Specify that PDP context requests that come in with a higher GBR value than the configured values are rejected, and PDP context requests that come in with a lower GBR value than the configured value are accepted:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set guaranteed-bit-rate-uplink 15000 reject
user@host# set guaranteed-bit-rate-downlink 25000 reject
```

6. Negotiate the uplink and downlink MBR for non-GBR PDP contexts by configuring each traffic class using the default, upgrade, or reject option.



**NOTE:** The following traffic classes are configured using the default (downgrade) behavior, which specifies that PDP context requests that come in with a lower MBR value than the configured value are upgraded to the configured MBR value, and PDP context requests that come in with a higher MBR value than the configured value are downgraded.

- a. Configure an MBR for the Interactive traffic class with Traffic Handling Priority (THP) 1 and signaling indication enabled:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set qci 5 maximum-bit-rate-uplink 10000
user@host# set qci 5 maximum-bit-rate-downlink 20000
```

- b. Configure an MBR for the Interactive traffic class with THP 1:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set qci 6 maximum-bit-rate-uplink 10000
user@host# set qci 6 maximum-bit-rate-downlink 20000
```

- c. Configure an MBR for Interactive traffic class with THP 2:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set qci 7 maximum-bit-rate-uplink 10000
user@host# set qci 7 maximum-bit-rate-downlink 20000
```

- d. Configure an MBR for Interactive traffic class with THP 3:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set qci 8 maximum-bit-rate-uplink 10000
user@host# set qci 8 maximum-bit-rate-downlink 20000
```

- e. Configure an MBR for the Background traffic class:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set qci 9 maximum-bit-rate-uplink 10000
user@host# set qci 9 maximum-bit-rate-downlink 10000
```

7. Configure the policer action to define how non-GBR bearer data should be treated when it exceeds the MBR value with which the PDP context was established.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 policer-action
non-ubr-bearer]
user@host# set violate-action set-loss-priority-high
```

When **violate-action** is configured with **set-loss-priority-high**, data that exceeds the MBR is transmitted with PLP high.



**NOTE:** By default, GTPv1 subscribers that exceed the MBR are dropped.

8. Configure the action to take when the GBR exceeds the GBR value with which the PDP context was established.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 policer-action gbr-bearer]
user@host# set exceed-action transmit
```



**NOTE:** By default, PDP contexts that exceed the GBR are set to PLP HIGH. When **exceed action** is configured with **transmit**, PDP contexts exceeding that GBR are transmitted with same PLP as PDP contexts within the GBR.

#### Related Documentation

- [Class of Service \(CoS\) Policy Profile Overview on page 508](#)
- [Configuring QoS on the Broadband Gateway Overview on page 516](#)
- [Configuring a CoS Policy Profile for 4G Networks on page 523](#)
- [Configuring a CoS Policy Profile for 3G and 4G Networks on page 531](#)
- [Example: Configuring Quality of Service on GGSN/P-GW on page 542](#)
- [Configuring S-GW-Specific CAC Parameters on page 581](#)
- [Example: Configuring QoS and CAC on a S-GW on page 582](#)



## Configuring a CoS Policy Profile for 3G and 4G Networks

In a 3G network, the class-of-service (CoS) policy profile defines the highest traffic class (mapped to QoS Class Identifier (QCI)) that can be accepted at an access point name (APN) or gateway level, the maximum bit rate (MBR) and guaranteed bit rate (GBR) for packet data protocol (PDP) contexts, and the allocation and retention priority (ARP). The CoS policy also specifies the policer actions when subscriber traffic exceeds the configured MBR and GBR values. By default, when a PDP context request has a higher MBR or GBR value than the value configured in the CoS policy profile, the MBR or GBR value of the PDP context request is downgraded.



**NOTE:** For GTPv1 subscribers, the MobileNext Broadband Gateway converts the traffic class to a QCI (as defined in the 3GPP specification 23.401 ANNEX E) and applies the CoS policy based on the configured QCI values.

In a 4G network, a CoS policy profile defines the highest QCI value that can be accepted at the APN level or gateway level, the aggregate maximum bit rate (AMBR) for default bearers, and the allocation and retention priority. By default, when a bearer request has a higher AMBR value than the value configured in the CoS policy profile, the AMBR value of bearer request is downgraded.

Before you begin, complete the following tasks:

- Configure a CoS classifier profile for 3G and 4G networks.
- Configure CoS bandwidth pools (for 3G networks only).
- Configure a CoS resource threshold profile for 3G and 4G networks.

To configure a CoS policy profile for 3G and 4G networks:

1. Specify a name for the CoS policy profile.

```
[edit unified-edge cos-cac]
user@host# edit cos-policy-profiles policy-profile-2
```

2. Negotiate the QCI value for 4G subscribers and the traffic class for 3G subscribers by doing one of the following:

- Downgrade the QCI value of create session requests that come in with a higher QCI value (numerically lower) than the configured value:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2]  
user@host# set default-bearer-qci 6
```



**NOTE:** When the default (downgrade) behavior is configured, if a create session request comes in with higher QCI value (numerically lower) than the value configured on the broadband gateway, the QCI value is downgraded to the configured value. If a create session request comes in with a lower QCI value (numerically higher) than the configured QCI, the QCI value is accepted.

- Upgrade the QCI value of create session requests that come in with a lower QCI value (numerically higher) than the configured value:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2]  
user@host# set default-bearer-qci 6 upgrade
```



**NOTE:** When the upgrade option is configured, if a create session request comes in with higher QCI value (numerically lower) than the value configured on the broadband gateway, the QCI value is downgraded to the configured value. If a create session request comes in with a lower QCI value (numerically higher) than the configured QCI, the QCI value is upgraded to the configured value.

- Reject the QCI value of create session requests that come in with a higher QCI value (numerically lower) than the configured value:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2]  
user@host# set default-bearer-qci 6 reject
```



**NOTE:** When the reject option is configured, if a create session request comes in with higher QCI value (numerically lower) than the value configured on the broadband gateway, the QCI value is rejected. If a create session request comes in with a lower QCI value (numerically higher) than the configured QCI, the QCI value is accepted as is.

3. Negotiate the ARP value for 3G and 4G subscribers when a PDP context or bearer is established or modified:

- Specify that bearers that come in with a lower ARP (numerically higher) than the configured value are accepted and bearers with a higher ARP (numerically lower) are downgraded to the configured value (default behavior):

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2]
```

```
user@host# set allocation-retention-priority 7
```

- Specify that bearers that come in with a lower ARP (numerically higher) than the configured value are accepted, and bearers with a higher ARP (numerically lower) are rejected:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2]
user@host# set allocation-retention-priority 7 reject
```



**NOTE:** For GTPv1 subscriber traffic received on the broadband gateway, ARP 1 maps to allocation-retention-priority 1, ARP 2 maps to allocation-retention-priority 6, and ARP 3 maps to allocation-retention-priority 11.



**NOTE:** If the allocation-retention-priority value is not specified, the broadband gateway uses the UE/SGSN requested or negotiated ARP value.

#### 4. Negotiate uplink and downlink AMBR for 4G subscribers by doing one of the following:

- Specify that bearer requests with an AMBR value higher than the configured value are downgraded to the configured AMBR value, and bearer requests with a lower value than the configured AMBR value are accepted (the default behavior):

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 aggregate-qos-control]
user@host# set maximum-bit-rate-uplink 15000
user@host# set maximum-bit-rate-downlink 25000
```

- Specify that bearer requests with a lower AMBR value than the configured value are upgraded to the configured AMBR value, and bearer requests with a higher AMBR value than the configured value are downgraded:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 aggregate-qos-control]
user@host# set maximum-bit-rate-uplink 15000 upgrade
user@host# set maximum-bit-rate-downlink 25000 upgrade
```

- Specify that bearer requests with a higher AMBR value than the configured value are rejected, and bearer requests with a lower AMBR value than the configured value are accepted:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 aggregate-qos-control]
user@host# set maximum-bit-rate-uplink 15000 reject
user@host# set maximum-bit-rate-downlink 25000 reject
```



**NOTE:** If the AMBR value is not specified, the broadband gateway uses the UE/MME requested or negotiated AMBR value.

5. Negotiate uplink and downlink MBR for 3G non-GBR PDP contexts by doing one of the following:

- Specify that PDP context requests that come in with an MBR value higher than the configured value are downgraded to the configured MBR value, and PDP context requests that come in with a lower value than the configured MBR value are accepted (the default behavior):

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set maximum-bit-rate-uplink 15000
user@host# set maximum-bit-rate-downlink 25000
```

- Specify that PDP context requests that come in with a lower MBR value than the configured value are upgraded to the configured MBR value, and PDP context requests that come in with a higher MBR values than the configured value are downgraded:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set maximum-bit-rate-uplink 15000 upgrade
user@host# set maximum-bit-rate-downlink 25000 upgrade
```

- Specify that PDP context requests that come in with a higher MBR value than the configured value are rejected, and PDP context requests that come in with a lower MBR value than the configured value are accepted:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set maximum-bit-rate-uplink 15000 reject
```

```
user@host# set maximum-bit-rate-downlink 25000 reject
```

6. Negotiate the uplink and downlink GBR for 3G GBR bearers by doing one of the following:

- Specify that PDP context requests that come in with a GBR value higher than the configured value are downgraded to the configured GBR value, and PDP context requests that come in with a lower value than the configured GBR value are accepted (the default behavior):

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set guaranteed-bit-rate-uplink 15000
user@host# set guaranteed-bit-rate-downlink 25000
```

- Specify that PDP context requests that come in with a lower GBR value than the configured value are upgraded to the configured GBR value, and PDP context requests that come in with a higher GBR value than the configured value are downgraded:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set guaranteed-bit-rate-uplink 15000 upgrade
user@host# set guaranteed-bit-rate-downlink 25000 upgrade
```

- Specify that PDP context requests that come in with a higher GBR value than the configured values are rejected, and PDP context requests that come in with a lower GBR value than the configured value are accepted:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set guaranteed-bit-rate-uplink 15000 reject
user@host# set guaranteed-bit-rate-downlink 25000 reject
```

7. Negotiate the uplink and downlink MBR for non-GBR PDP contexts, you configure each traffic class using either the default, upgrade, or reject behavior.



**NOTE:** The following traffic classes are configured using the default (downgrade) behavior. PDP context requests that come in with a lower MBR value than the configured value are upgraded to the configured MBR value, and PDP context requests that come in with a higher MBR value than the configured value are downgraded.

- a. Configure an MBR for the Interactive traffic class with Traffic Handling Priority (THP) 1 and signaling indication enabled:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set qci 5 maximum-bit-rate-uplink 10000
user@host# set qci 5 maximum-bit-rate-downlink 20000
```

- b. Configure an MBR for the Interactive traffic class with THP 1:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set qci 6 maximum-bit-rate-uplink 10000
user@host# set qci 6 maximum-bit-rate-downlink 20000
```

- c. Configure an MBR for Interactive traffic class with THP 2:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set qci 7 maximum-bit-rate-uplink 10000
user@host# set qci 7 maximum-bit-rate-downlink 20000
```

- d. Configure an MBR for Interactive traffic class with THP 3:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set qci 8 maximum-bit-rate-uplink 10000
user@host# set qci 8 maximum-bit-rate-downlink 20000
```

- e. Configure an MBR for the Background traffic class:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 pdp-qos-control]
user@host# set qci 9 maximum-bit-rate-uplink 10000
user@host# set qci 9 maximum-bit-rate-downlink 10000
```

8. Configure the policer action to define how non-GBR bearer data is treated when it exceeds the MBR value with which the PDP context was established or the AMBR value with which the default bearer was established.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 policer-action
non-ubr-bearer]
user@host# set violate-action set-loss-priority-high
```

When **violate-action** is configured with **set-loss-priority-high**, data that exceeds the MBR is transmitted with PLP high.



**NOTE:** By default, GTPv1 subscribers that exceed the MBR and GTPv2 subscribers that exceed the AMBR are dropped.

9. Configure the policer actions to take to define how GBR bearer data is treated:

- a. Configure the policer action to define how GBR bearer data is treated when the MBR exceeds the MBR value with which the PDP context was established.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 policer-action
non-ubr-bearer]
user@host# set violate-action set-loss-priority-high
```

- b. Configure the policer actions to take to define how GBR bearer data is treated when the GBR exceeds the GBR value with which the PDP context was established.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 policer-action
ubr-bearer]
user@host# set exceed-action transmit
```



**NOTE:** By default, PDP contexts that exceed the GBR are set to PLP HIGH. When **exceed** action is configured with **transmit**, PDP contexts exceeding the GBR are transmitted with the same PLP as PDP contexts within the GBR.

- [Configuring QoS on the Broadband Gateway Overview on page 516](#)
- [Configuring S-GW-Specific CAC Parameters on page 581](#)
- [Example: Configuring QoS and CAC on a S-GW on page 582](#)

## Configuring a Local Policy

A local policy defines the quality-of-service (QoS) treatment to be applied at the system level or access point name (APN) level for the MobileNext Broadband Gateway. A local policy applied at the APN level takes priority over a local policy applied at the system level. A local policy defines traffic by classes and specifies the different levels of throughput and packet loss when congestion occurs.

Before you begin, configure each of the following QoS features:

- **Bandwidth pool**—Limits the GBR bandwidth usage at the system level or APN level. The broadband gateway's call admission control (CAC) uses bandwidth pools to negotiate and reserve bandwidth.
- **Resource threshold profiles**—Limit CPU and memory load. When the number of bearers or system load (memory, CPU, and queue depth) reaches a configured low or high threshold, only higher-priority bearer requests are allowed.
- **Classifier profiles**—Define the mapping of traffic classes (a traffic class or QoS Class Identifier [QCI]) to a forwarding class and packet loss priority (PLP). You configure separate classifier profiles for home, roaming, and visitor subscriber traffic.
- **CoS policy profiles**—Configure separate class-of-service (CoS) profiles for home, roaming, and visitor subscriber traffic.

To configure a local policy:

1. Specify a name for the local policy.

```
[edit unified-edge]
user@host# edit local-policies local-policy-2
```

2. Specify the classifier profiles to include in the local policy to define the mapping of each traffic class to a forwarding class and PLP.

```
[edit unified-edge local-policies local-policy-2]
user@host# set classifier-profile home-classifier-profile-1
user@host# set roamer-classifier-profile roaming-classifier-profile-1
user@host# set visitor-classifier-profile visiting-classifier-profile-1
```

3. Specify the CoS policy profiles to include in the local policy to define the QoS parameters for bearer setup and teardown.

```
[edit unified-edge local-policies local-policy-2]
user@host# set policy-profile home-policy-profile-1
user@host# set roamer-policy-profile roaming-policy-profile-1
user@host# set visitor-policy-profile visiting-policy-profile-1
```

4. Specify the resource threshold profile to include in the local policy to define admission control for managing system overload conditions.

```
[edit unified-edge local-policies local-policy-2]  
user@host# set resource-threshold-profiles resource-threshold--profile-1
```

5. Specify a bandwidth pool for downlink traffic.

```
[edit unified-edge local-policies local-policy-2]  
user@host# set dl-bandwidth-pool bw-pool-downlink-1
```

6. Specify a bandwidth pool for uplink traffic.

```
[edit unified-edge local-policies local-policy-2]  
user@host# set ul-bandwidth-pool bw-pool-uplink-1
```

**Related  
Documentation**

- [Configuring QoS on the Broadband Gateway Overview on page 516](#)
- [Configuring the Maximum Number of Bearers on page 517](#)
- [Configuring Bandwidth Pools on page 518](#)
- [Configuring S-GW-Specific CAC Parameters on page 581](#)
- [Example: Configuring QoS and CAC on a S-GW on page 582](#)

---

## Applying a Local Policy

A local policy defines the QoS treatment to be applied at the system level or access point name (APN) level for a MobileNext Broadband Gateway. A local policy applied at the APN level takes priority over a local policy applied at the system level.

Before you begin, you must configure a local policy to define the QoS treatment to be applied at the system level or APN level for a broadband gateway.

- To apply a local policy at the system level:

```
[edit gateways ggsn-pgw MBG1]  
user@host# edit local-policy-profile local-policy1
```

- To apply a local policy at the access point name (APN) level:

```
[edit gateways ggsn-pgw MBG1 apn-services apns apn1]  
user@host# edit local-policy-profile local-policy2
```

**Related  
Documentation**

- [Configuring a Local Policy on page 537](#)
- [Configuring the Maximum Number of Bearers on page 517](#)
- [Configuring Bandwidth Pools on page 518](#)
- [Configuring QoS on the Broadband Gateway Overview on page 516](#)
- [Configuring S-GW-Specific CAC Parameters on page 581](#)
- [Example: Configuring QoS and CAC on a S-GW on page 582](#)



## Configuring Ingress Rewrite Rules for a Mobile Interface

You configure egress rewrite rules and then apply those rules to change DiffServ code point (DSCP) bits or IP precedence bits for subscriber packets received on a mobile interface.

To create an ingress rewrite rule for a mobile interface:

1. Specify a name for the ingress rewrite rules.

```
[edit class-of-service rewrite-rules]
user@host# edit dscp dscp_v4_ingress_rw
```

2. Configure a rewrite rules mapping on DSCP, DSCP IPv6, or IP precedence values; for example:

```
[edit class-of-service rewrite-rules dscp dscp_v4_ingress_rw]
user@host# set forwarding class af1 loss-priority high code-point 001110
user@host# set forwarding class af1 loss-priority low code-point 001010
user@host# set forwarding class af2 loss-priority high code-point 010110
user@host# set forwarding class af2 loss-priority low code-point 010010
user@host# set forwarding class af3 loss-priority high code-point 011110
user@host# set forwarding class af3 loss-priority low code-point 011010
user@host# set forwarding class af4 loss-priority high code-point 100110
user@host# set forwarding class af4 loss-priority low code-point 100010
user@host# set forwarding class be loss-priority low code-point 000000
```

### Related Documentation

- [Applying Rewrite Rules on Mobile Interfaces Overview on page 510](#)
- [Configuring Egress Rewrite Rules for a Mobile Interface on page 539](#)
- [Configuring QoS on the Broadband Gateway Overview on page 516](#)
- [Configuring S-GW-Specific CAC Parameters on page 581](#)
- [Example: Configuring QoS and CAC on a S-GW on page 582](#)

## Configuring Egress Rewrite Rules for a Mobile Interface

You configure egress rewrite rules and then apply those rules to change DiffServ code point (DSCP) bits or IP precedence bits for subscriber packets received on a mobile interface.

To create an egress rewrite rule for a mobile interface:

1. Specify a name for the egress rewrite rules.

```
[edit class-of-service rewrite-rules]
user@host# edit dscp dscp_v4_egress_rw
```

2. Configure a rewrite rules mapping on DSCP, DSCP IPv6, or IP precedence values; for example:

```
[edit class-of-service rewrite-rules dscp dscp_v4_egress_rw]
user@host# set forwarding class af1 loss-priority high code-point 001110
```

```
user@host# set forwarding class af1 loss-priority low code-point 001010
user@host# set forwarding class af2 loss-priority high code-point 010110
user@host# set forwarding class af2 loss-priority low code-point 010010
user@host# set forwarding class af3 loss-priority high code-point 011110
user@host# set forwarding class af3 loss-priority low code-point 011010
user@host# set forwarding class af4 loss-priority high code-point 100110
user@host# set forwarding class af4 loss-priority low code-point 100010
user@host# set forwarding class be loss-priority low code-point 000000
```

**Related Documentation**

- [Applying Rewrite Rules on Mobile Interfaces Overview on page 510](#)
- [Configuring QoS on the Broadband Gateway Overview on page 516](#)
- [Configuring Ingress Rewrite Rules for a Mobile Interface on page 539](#)
- [Configuring S-GW-Specific CAC Parameters on page 581](#)
- [Example: Configuring QoS and CAC on a S-GW on page 582](#)

---

## Applying Ingress Rewrite Rules to a Mobile Interface

You apply ingress rewrite rules to change the DiffServ code point (DSCP), DSCPv6, or IP precedence value in the IP header of the upstream subscriber packets. You can specify rewrite rules for DSCPv4, DSCPv6, or IP precedence values.

The rewrite rule is applied for Gn-to-Gi traffic at the mobile interface and rewrites into the outer IP header of the subscriber packet only.



**NOTE:** DSCP marking on the subscriber packet is required for mobile traffic. If ingress rewrite rules are not configured and applied to the mif interface, the default `mcos-dscp-default` or `mcos-dscpv6-default` rewrite rules apply.

Before you begin, complete the following tasks:

- Configure an ingress rewrite rule.
- Configure the mobile interfaces.

To apply a rewrite rule to the outer IP header, specify the name of the rewrite rule that you want to apply to the mobile interface; for example:

```
[edit class-of-service interfaces mif unit 0 ingress-rewrite-rules]
user@host# set dscp uplink_rewrite_v4_dscp
```

**Related Documentation**

- [Applying Rewrite Rules on Mobile Interfaces Overview on page 510](#)
- [Configuring QoS on the Broadband Gateway Overview on page 516](#)
- [Applying Egress Rewrite Rules to Mobile Interfaces on page 541](#)
- [Configuring S-GW-Specific CAC Parameters on page 581](#)
- [Example: Configuring QoS and CAC on a S-GW on page 582](#)

## Applying Egress Rewrite Rules to Mobile Interfaces

You apply egress rewrite rules to change the DiffServ code point (DSCP), DSCPv6, or IP precedence value in the IP header of downstream subscriber packets. You can specify rewrite rules for DSCPv4, DSCPv6, or IP precedence values.

An egress rewrite rule for downstream (Gi-to-Gn or SGi-to-S5) traffic is applied at the mobile interface and rewrites into the inner IP header, and optionally, outer IP header, or both inner and outer IP headers.



**NOTE:** DSCP marking on the subscriber packet is required for mobile traffic. If egress rewrite rules are not configured and applied to the mobile interfaces, the default `mcos-dscp-default` or `mcos-dscpv6-default` rewrite rules apply.

Before you begin, complete the following tasks:

- Configure the mobile interfaces.
- Configure an egress rewrite rule.

To apply an egress rewrite rule to change DSCP, DSCPv6, or IP precedence values in the IP header of downstream subscriber packets:

- To apply a DSCP (IPv4) rewrite rule to the inner IP header, specify the name of the rewrite rule you want to apply to the mobile interface.

```
[edit class-of-service interfaces mif unit 0 rewrite-rules]
user@host# set dscp downlink_rewrite_v4_dscp_inner
```

- To apply a rewrite rule on the outer IP header, specify the name of the rewrite rule you want to apply to the mobile interface and include the **gtp-inet-outer** option.

```
[edit class-of-service interfaces mif unit 0 rewrite-rules]
user@host# set dscp downlink_rewrite_v4_dscp_outer protocol gtp-inet-outer
```

- To apply a DSCP rewrite rule to both the inner and outer IP headers, specify the name of the rewrite rule you want to apply to the mobile interface and include the **gtp-inet-both** option.

```
[edit class-of-service interfaces mif unit 0 rewrite-rules]
user@host# set dscp downlink_rewrite_v4_dscp protocol gtp-inet-both
```

### Related Documentation

- [Applying Rewrite Rules on Mobile Interfaces Overview on page 510](#)
- [Configuring QoS on the Broadband Gateway Overview on page 516](#)
- [Applying Ingress Rewrite Rules to a Mobile Interface on page 540](#)

## Example: Configuring Quality of Service on GGSN/P-GW

---

This example describes how to configure quality of service (QoS) on the MobileNext Broadband Gateway, and consists of the following sections:

- [Requirements on page 542](#)
- [Overview on page 543](#)
- [Configuration on page 544](#)
- [Verification on page 575](#)

### Requirements

This example uses the following hardware and software components:

- An operational MX Series chassis
- Junos OS MobileNext Broadband Gateway software package

Before you begin:

- Configure mobile interfaces for access point names (APNs)
- Configure APNs on the broadband gateway
- Configure Junos OS class-of-service (CoS) forwarding classes

## Overview

In a mobile network, the availability of network resources is shared among multiple services (including Internet, voice, video, e-mail, and file sharing), each of which has different QoS requirements in terms of required bit rates, acceptable packet loss rates, and packet delay. You configure QoS on the broadband gateway to prioritize subscriber traffic and provide better service to certain services or subscribers to the detriment of other services and subscribers.

To configure QoS on the broadband gateway, you create a set of QoS profiles that are then referenced in a local policy, which defines the QoS treatment for 3G 4G subscriber traffic on the broadband gateway. You configure the following profiles and policies:

- **Classifier profiles**—Define the mapping of each traffic class and QoS Class Identifier (QCI) to a forwarding class and packet loss priority. You configure a separate classifier profiles for home, visiting, and roaming subscribers on 3G and 4G networks. Each classifier profile uses a GTPv2 QCI to define forwarding treatment for 3G and 4G subscribers. For 3G subscribers, the broadband gateway maps the GTPv1 traffic class or traffic handling priorities to the equivalent GTPv2 QCI and applies the classification. For example, a GTPv1 subscriber that arrives on the gateway with Interactive traffic class and THP 1 and signaling indication enabled maps to QCI 5, and data for this subscriber is classified based on the QCI 5 forwarding treatment you configure in the classifier profile. For information about mapping of QCI values to Release 99 QoS parameter values, see the [“Quality of Service Overview” on page 499](#).
- **Resource threshold profiles**—Define the thresholds for number of bearers, memory, and CPU load. Call admission control (CAC) is based on the configured resource thresholds and allows only higher priority traffic when low or high resource thresholds are exceeded. You can configure a single resource threshold profile at the gateway level for 3G and 4G subscribers.
- **CoS policy profiles**—Define the negotiation of QoS parameters to determine when bearer requests can be upgraded, downgraded, or rejected. You define CoS policy profiles to provide separate QoS configurations for home, visiting, and roaming subscribers on 3G and 4G networks.
- **Bandwidth pools**—Define bandwidth pools to limit guaranteed bit rate (GBR) utilization (3G networks).
- **Local policies**—Define the overall CoS and call admission control behavior for 3G and 4G subscriber traffic. A local policy is applied at either the gateway or access point name (APN) level. A local policy applied at the APN level takes priority over a local policy applied at the gateway. Each local policy includes the classifier profiles, resource threshold profiles, and CoS policy profiles that define the overall QoS treatment for 3G subscriber traffic, 4G subscriber traffic, or both. A local policy can include multiple classifier profiles, resource threshold profiles, and CoS policy profiles to provide QoS treatment specific to the home, visiting, and roaming subscribers on 3G and 4G networks.
- **Rewrite rules**—Provide the required DiffServ code point (DSCP) marking of subscriber packets for uplink and downlink traffic.

## Configuration

To configure QoS on the broadband gateway, perform the following tasks:

- [Configuring Classifier Profiles for Home Subscribers on 3G and 4G Networks on page 544](#)
- [Configuring Classifier Profiles for Roaming Subscribers on 3G and 4G Networks on page 545](#)
- [Configuring Classifier Profiles for Visitor Subscribers on 3G and 4G Networks on page 546](#)
- [Configuring a System-Wide Classifier Profile on page 547](#)
- [Configuring a System-Wide Resource Threshold Profile on page 548](#)
- [Configuring a CoS Policy Profile for Home Subscribers on a 3G Network on page 549](#)
- [Configuring a CoS Policy Profile for Home Subscribers on a 4G Network on page 552](#)
- [Configuring a CoS Policy Profile for Roaming Subscribers on a 3G Network on page 553](#)
- [Configuring a CoS Policy Profile for Roaming Subscribers on a 4G Network on page 556](#)
- [Configuring a CoS Policy Profile for Visiting Subscribers on a 3G Network on page 557](#)
- [Configuring a CoS Policy Profile for Visiting Subscribers on a 4G Network on page 560](#)
- [Configuring a System-Wide CoS Policy Profile on page 561](#)
- [Configuring Bandwidth Pools on page 564](#)
- [Configuring a Local Policy for 3G Networks on page 565](#)
- [Configuring a Local Policy for 4G Networks on page 566](#)
- [Configuring a System-Wide Local Policy on page 567](#)
- [Applying the Local Policies on page 568](#)
- [Configuring DSCP Ingress Rewrite Rules for IPv4 Packets on page 569](#)
- [Configuring DSCP Ingress Rewrite Rules for IPv6 Packets on page 570](#)
- [Configuring DSCP Egress Rewrite Rules for IPv4 Packets on page 571](#)
- [Configuring DSCP Egress Rewrite Rules for IPv6 Packets on page 572](#)
- [Applying Ingress Rewrite Rules to Mobile Interfaces for 3G and 4G Subscriber Traffic on page 573](#)
- [Applying Egress Rewrite Rules to Mobile Interfaces for 3G and 4G Subscriber Traffic on page 573](#)
- [Configuring the Maximum Number of Bearers on page 574](#)
- [Enabling Preemption on page 574](#)

---

### Configuring Classifier Profiles for Home Subscribers on 3G and 4G Networks

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge cos-cac classifier-profiles home_pgw qos-class-identifier 2
  forwarding-class af1 loss-priority low
set unified-edge cos-cac classifier-profiles home_pgw qos-class-identifier 4
  forwarding-class af2 loss-priority low
```

```

set unified-edge cos-cac classifier-profiles home_pgw qos-class-identifier 5
  forwarding-class af1 loss-priority low
set unified-edge cos-cac classifier-profiles home_pgw qos-class-identifier 6
  forwarding-class af2 loss-priority low
set unified-edge cos-cac classifier-profiles home_pgw qos-class-identifier 7
  forwarding-class af3 loss-priority low
set unified-edge cos-cac classifier-profiles home_pgw qos-class-identifier 8
  forwarding-class af4 loss-priority low
set unified-edge cos-cac classifier-profiles home_pgw qos-class-identifier 9
  forwarding-class af4 loss-priority low

```

### Step-by-Step Procedure

To configure a classifier profile for home subscribers on 3G and 4G Networks:

1. Specify a name for the home classifier profile and map each 3G traffic class and 4G QoS Class Identifier to a forwarding class and packet loss priority.

[edit]

```

user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_pgw
  qos-class-identifier 2 forwarding-class af1 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_pgw
  qos-class-identifier 4 forwarding-class af2 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_pgw
  qos-class-identifier 5 forwarding-class af1 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_pgw
  qos-class-identifier 6 forwarding-class af2 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_pgw
  qos-class-identifier 7 forwarding-class af3 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_pgw
  qos-class-identifier 8 forwarding-class af4 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_pgw
  qos-class-identifier 9 forwarding-class af4 loss-priority low

```

**Results** From configuration mode, confirm your configuration by entering the **show** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

### Configuring Classifier Profiles for Roaming Subscribers on 3G and 4G Networks

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

[edit]

```

set unified-edge cos-cac classifier-profiles roamer_pgw qos-class-identifier 2
  forwarding-class af1 loss-priority high
set unified-edge cos-cac classifier-profiles roamer_pgw qos-class-identifier 4
  forwarding-class af2 loss-priority high
set unified-edge cos-cac classifier-profiles roamer_pgw qos-class-identifier 5
  forwarding-class af3 loss-priority low
set unified-edge cos-cac classifier-profiles roamer_pgw qos-class-identifier 6
  forwarding-class af4 loss-priority low
set unified-edge cos-cac classifier-profiles roamer_pgw qos-class-identifier 7
  forwarding-class af4 loss-priority low

```

```
set unified-edge cos-cac classifier-profiles roamer_pgw qos-class-identifier 8
forwarding-class ef loss-priority high
set unified-edge cos-cac classifier-profiles roamer_pgw qos-class-identifier 9
forwarding-class be loss-priority high
```

**Step-by-Step  
Procedure**

To configure classifier profiles for roaming subscribers on 3G and 4G networks:

1. Specify a name for the roamer classifier profile and map each 3G traffic class and 4G QoS Class Identifier to a forwarding class and packet loss priority.

[edit]

```
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_pgw
qos-class-identifier 2 forwarding-class af1 loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_pgw
qos-class-identifier 4 forwarding-class af2 loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_pgw
qos-class-identifier 5 forwarding-class af3 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_pgw
qos-class-identifier 6 forwarding-class af4 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_pgw
qos-class-identifier 7 forwarding-class af4 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_pgw
qos-class-identifier 8 forwarding-class ef loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_pgw
qos-class-identifier 9 forwarding-class be loss-priority high
```

### Configuring Classifier Profiles for Visitor Subscribers on 3G and 4G Networks

**CLI Quick  
Configuration**

To quickly configure this example, copy the following commands and paste them into the router terminal window:

[edit]

```
set unified-edge cos-cac classifier-profiles visitor_pgw qos-class-identifier 2
forwarding-class af1 loss-priority high
set unified-edge cos-cac classifier-profiles visitor_pgw qos-class-identifier 4
forwarding-class af2 loss-priority high
set unified-edge cos-cac classifier-profiles visitor_pgw qos-class-identifier 5
forwarding-class af4 loss-priority high
set unified-edge cos-cac classifier-profiles visitor_pgw qos-class-identifier 6
forwarding-class af4 loss-priority high
set unified-edge cos-cac classifier-profiles visitor_pgw qos-class-identifier 7
forwarding-class ef loss-priority high
set unified-edge cos-cac classifier-profiles visitor_pgw qos-class-identifier 8
forwarding-class be loss-priority high
set unified-edge cos-cac classifier-profiles visitor_pgw qos-class-identifier 9
forwarding-class nc loss-priority high
```

**Step-by-Step  
Procedure**

To configure classifier profiles for visitor subscribers on 3G and 4G networks:

1. Specify a name for the visitor classifier profile and map each 3G traffic class and 4G QoS Class Identifier to a forwarding class and packet loss priority.

[edit]

```
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_pgw
qos-class-identifier 2 forwarding-class af1 loss-priority high
```



```

user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_pgw
qos-class-identifier 4 forwarding-class af2 loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_pgw
qos-class-identifier 5 forwarding-class af4 loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_pgw
qos-class-identifier 6 forwarding-class af4 loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_pgw
qos-class-identifier 7 forwarding-class ef loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_pgw
qos-class-identifier 8 forwarding-class be loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_pgw
qos-class-identifier 9 forwarding-class nc loss-priority high

```

### Configuring a System-Wide Classifier Profile

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```

[edit]
set unified-edge cos-cac classifier-profiles system_wide qos-class-identifier 2
forwarding-class af2 loss-priority low
set unified-edge cos-cac classifier-profiles system_wide qos-class-identifier 4
forwarding-class af3 loss-priority low
set unified-edge cos-cac classifier-profiles system_wide qos-class-identifier 5
forwarding-class af4 loss-priority low
set unified-edge cos-cac classifier-profiles system_wide qos-class-identifier 6
forwarding-class af4 loss-priority high
set unified-edge cos-cac classifier-profiles system_wide qos-class-identifier 7
forwarding-class nc loss-priority high
set unified-edge cos-cac classifier-profiles system_wide qos-class-identifier 8
forwarding-class ef loss-priority high
set unified-edge cos-cac classifier-profiles system_wide qos-class-identifier 9
forwarding-class be loss-priority high

```

#### Step-by-Step Procedure

To configure the system-wide classifier profile for 3G and 4G networks:

1. Specify a name (**system\_wide**) for the classifier profile and map each 3G traffic class and 4G QoS Class Identifier to a forwarding class and packet loss priority.

```

[edit]
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles system_wide
qos-class-identifier 2 forwarding-class af2 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles system_wide
qos-class-identifier 4 forwarding-class af3 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles system_wide
qos-class-identifier 5 forwarding-class af4 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles system_wide
qos-class-identifier 6 forwarding-class af4 loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles system_wide
qos-class-identifier 7 forwarding-class nc loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles system_wide
qos-class-identifier 8 forwarding-class ef loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles system_wide
qos-class-identifier 9 forwarding-class be loss-priority high

```

**Results** From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

---

### Configuring a System-Wide Resource Threshold Profile

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge cos-cac resource-threshold-profiles resource_pgw bearers-load low
percentage 60
set unified-edge cos-cac resource-threshold-profiles resource_pgw bearers-load low
priority-level 7
set unified-edge cos-cac resource-threshold-profiles resource_pgw bearers-load high
percentage 80
set unified-edge cos-cac resource-threshold-profiles resource_pgw bearers-load high
priority-level 4
set unified-edge cos-cac resource-threshold-profiles resource_pgw cpu low percentage
70
set unified-edge cos-cac resource-threshold-profiles resource_pgw cpu low priority-level
7
set unified-edge cos-cac resource-threshold-profiles resource_pgw cpu high percentage
80
set unified-edge cos-cac resource-threshold-profiles resource_pgw cpu high priority-level
4
set unified-edge cos-cac resource-threshold-profiles resource_pgw memory low percentage
85
set unified-edge cos-cac resource-threshold-profiles resource_pgw memory low
priority-level 10
set unified-edge cos-cac resource-threshold-profiles resource_pgw memory high percentage
90
set unified-edge cos-cac resource-threshold-profiles resource_pgw memory high
priority-level 5
```

**Step-by-Step Procedure** To configure resource threshold profiles for subscribers on 3G and 4G networks:

1. Configure the low and high thresholds for bearer load.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_pgw
bearers-load low percentage 60
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_pgw
bearers-load low priority-level 7
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_pgw
bearers-load high percentage 80
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_pgw
bearers-load high priority-level 4
```

2. Configure the low and high thresholds for the CPU load.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_pgw
cpu low percentage 70
```

```

user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_pgw
cpu low priority-level 7
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_pgw
cpu high percentage 80
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_pgw
cpu high priority-level 4

```

3. Configure the low and high thresholds for the memory load.

```

[edit]
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_pgw
memory low percentage 85
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_pgw
memory low priority-level 10
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_pgw
memory high percentage 90
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_pgw
memory high priority-level 5

```

**Results** From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

### Configuring a CoS Policy Profile for Home Subscribers on a 3G Network

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```

[edit]
set unified-edge cos-cac cos-policy-profiles home_v1 default-bearer-qci 6 upgrade
set unified-edge cos-cac cos-policy-profiles home_v1 allocation-retention-priority 5
set unified-edge cos-cac cos-policy-profiles home_v1 pdp-qos-control
maximum-bit-rate-uplink 3072 upgrade
set unified-edge cos-cac cos-policy-profiles home_v1 pdp-qos-control
maximum-bit-rate-downlink 3072 upgrade
set unified-edge cos-cac cos-policy-profiles home_v1 pdp-qos-control
guaranteed-bit-rate-uplink 3008 upgrade
set unified-edge cos-cac cos-policy-profiles home_v1 pdp-qos-control
guaranteed-bit-rate-downlink 3008 upgrade
set unified-edge cos-cac cos-policy-profiles home_v1 pdp-qos-control qci 6
maximum-bit-rate-uplink 896
set unified-edge cos-cac cos-policy-profiles home_v1 pdp-qos-control qci 6
maximum-bit-rate-downlink 896
set unified-edge cos-cac cos-policy-profiles home_v1 pdp-qos-control qci 7
maximum-bit-rate-uplink 896
set unified-edge cos-cac cos-policy-profiles home_v1 pdp-qos-control qci 7
maximum-bit-rate-downlink 896
set unified-edge cos-cac cos-policy-profiles home_v1 pdp-qos-control qci 8
maximum-bit-rate-uplink 896
set unified-edge cos-cac cos-policy-profiles home_v1 pdp-qos-control qci 8
maximum-bit-rate-downlink 896
set unified-edge cos-cac cos-policy-profiles home_v1 pdp-qos-control qci 9
maximum-bit-rate-uplink 896

```

```

set unified-edge cos-cac cos-policy-profiles home_v1 pdp-qos-control qci 9
maximum-bit-rate-downlink 896
set unified-edge cos-cac cos-policy-profiles home_v1 policer-action non-gbr-bearer
violate-action transmit
set unified-edge cos-cac cos-policy-profiles home_v1 policer-action gbr-bearer
exceed-action transmit
set unified-edge cos-cac cos-policy-profiles home_v1 policer-action gbr-bearer
violate-action transmit

```

### Step-by-Step Procedure

To configure a CoS policy profile for home subscribers in a 3G network:

1. Specify a name for the CoS policy profile, negotiate the non-GBR traffic class for 3G subscribers, and specify the **upgrade** option to upgrade the traffic class (mapped to QCI value) of create PDP context requests that come in with a lower traffic class than the configured value and downgrade requests with a higher traffic class (numerically lower QCI value):

[edit]

```

user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
default-bearer-qci 6 upgrade

```

2. Specify that PDP context requests that come in with a lower ARP (numerically higher) than the configured value are accepted and PDP context requests with a higher ARP (numerically lower) are downgraded to the configured value (default behavior).

[edit]

```

user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
allocation-retention-priority 5

```



**NOTE:** For GTPv1 subscriber traffic received on the broadband gateway, ARP 1 maps to allocation-retention-priority 1, ARP 2 maps to allocation-retention-priority 6, and ARP 3 maps to allocation-retention-priority 11.



**NOTE:** If the allocation-retention-priority value is not specified, the broadband gateway uses the UE/SGSN requested or negotiated ARP value.

3. Specify that GBR PDP context requests that come in with a lower MBR value than the configured value are upgraded to the configured MBR value, and PDP context requests that come in with a higher MBR values than the configured value are downgraded to the configured MBR value.

[edit]

```

user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
pdp-qos-control maximum-bit-rate-uplink 3072 upgrade
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
pdp-qos-control maximum-bit-rate-downlink 3072 upgrade

```

4. Specify that GBR PDP context requests that come in with a lower GBR value than the configured value are upgraded to the configured GBR value, and PDP context requests that come in with a higher GBR value than the configured value are downgraded to the configured GBR value.

```
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
pdp-qos-control guaranteed-bit-rate-uplink 3008 upgrade
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
pdp-qos-control guaranteed-bit-rate-downlink 3008 upgrade
```

5. Configure the uplink and downlink maximum bit rates for the non-GBR traffic classes:
  - a. Configure an MBR for the Interactive traffic class with THP 1 (without signaling indication):

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
pdp-qos-control qci 6 maximum-bit-rate-uplink 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
pdp-qos-control qci 6 maximum-bit-rate-downlink 896
```

- b. Configure an MBR for the Interactive traffic class with THP 2:

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
pdp-qos-control qci 7 maximum-bit-rate-uplink 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
pdp-qos-control qci 7 maximum-bit-rate-downlink 896
```

- c. Configure an MBR for the Interactive traffic class with THP 3:

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
pdp-qos-control qci 8 maximum-bit-rate-uplink 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
pdp-qos-control qci 8 maximum-bit-rate-downlink 896
```

- d. Configure an MBR for the Background traffic class:

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
pdp-qos-control qci 9 maximum-bit-rate-uplink 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
pdp-qos-control qci 9 maximum-bit-rate-downlink 896
```

6. Configure the action to take for non-GBR PDP context requests when the MBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1 policer-action
non-gbr-bearer violate-action transmit
```

7. Configure the action to take for GBR PDP context requests when the GBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1 policer-action
gbr-bearer exceed-action transmit
```

8. Configure the action to take for GBR PDP context requests when the MBR exceeds the configured value.

[edit]

```
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1 policer-action
gbr-bearer violate-action transmit
```

**Results** From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

### Configuring a CoS Policy Profile for Home Subscribers on a 4G Network

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

[edit]

```
set unified-edge cos-cac cos-policy-profiles home_v2 default-bearer-qci 6 upgrade
set unified-edge cos-cac cos-policy-profiles home_v2 allocation-retention-priority 5 upgrade
set unified-edge cos-cac cos-policy-profiles home_v2 aggregate-qos-control
maximum-bit-rate-uplink 2048
set unified-edge cos-cac cos-policy-profiles home_v2 aggregate-qos-control
maximum-bit-rate-downlink 2048
set unified-edge cos-cac cos-policy-profiles home_v2 policer-action non-gbr-bearer
violate-action transmit
```

**Step-by-Step Procedure** To configure a CoS policy profile for home subscribers in a 4G network:

1. Specify a name for the CoS policy profile, negotiate the QoS Class Identifier (QCI) for 4G subscribers, and specify the **upgrade** option to upgrade the QCI value of bearer requests that come in with a lower QCI (numerically higher) than the configured value and downgrade requests with a higher QCI.

[edit]

```
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v2
default-bearer-qci 6 upgrade
```

2. Specify that bearers that come in with a lower ARP (numerically higher) than the configured value are accepted and bearers with a higher ARP (numerically lower) are downgraded to the configured value (default behavior).

[edit]

```
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v2
allocation-retention-priority 5
```



**NOTE:** If the allocation-retention-priority value is not specified, the broadband gateway uses the UE/SGW requested or negotiated ARP value.

- Specify that bearers that come in with a lower MBR value than the configured value are upgraded to the configured MBR value, and bearers that come in with a higher MBR values than the configured value are downgraded to the configured MBR value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v2
  aggregate-qos-control maximum-bit-rate-uplink 2048
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v2
  aggregate-qos-control maximum-bit-rate-downlink 2048
```

- Configure the action to take for bearers when the AMBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v2
  policer-action non-gbr-bearer violate-action transmit
```

**Results** From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

### Configuring a CoS Policy Profile for Roaming Subscribers on a 3G Network

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge cos-cac cos-policy-profiles roamer_v1 default-bearer-qci 6
set unified-edge cos-cac cos-policy-profiles roamer_v1 allocation-retention-priority 6
set unified-edge cos-cac cos-policy-profiles roamer_v1 pdp-qos-control
  maximum-bit-rate-uplink 2500
set unified-edge cos-cac cos-policy-profiles roamer_v1 pdp-qos-control
  maximum-bit-rate-downlink 2500
set unified-edge cos-cac cos-policy-profiles roamer_v1 pdp-qos-control
  guaranteed-bit-rate-uplink 2372
set unified-edge cos-cac cos-policy-profiles roamer_v1 pdp-qos-control
  guaranteed-bit-rate-downlink 2372
set unified-edge cos-cac cos-policy-profiles roamer_v1 pdp-qos-control qci 6
  maximum-bit-rate-uplink 896
set unified-edge cos-cac cos-policy-profiles roamer_v1 pdp-qos-control qci 6
  maximum-bit-rate-downlink 896
set unified-edge cos-cac cos-policy-profiles roamer_v1 pdp-qos-control qci 7
  maximum-bit-rate-uplink 896
set unified-edge cos-cac cos-policy-profiles roamer_v1 pdp-qos-control qci 7
  maximum-bit-rate-downlink 896
set unified-edge cos-cac cos-policy-profiles roamer_v1 pdp-qos-control qci 8
  maximum-bit-rate-uplink 896
set unified-edge cos-cac cos-policy-profiles roamer_v1 pdp-qos-control qci 8
  maximum-bit-rate-downlink 896
set unified-edge cos-cac cos-policy-profiles roamer_v1 pdp-qos-control qci 9
  maximum-bit-rate-uplink 896
set unified-edge cos-cac cos-policy-profiles roamer_v1 pdp-qos-control qci 9
  maximum-bit-rate-downlink 896
```

```

set unified-edge cos-cac cos-policy-profiles roamer_v1 policer-action non-gbr-bearer
violate-action transmit
set unified-edge cos-cac cos-policy-profiles roamer_v1 policer-action gbr-bearer
exceed-action transmit
set unified-edge cos-cac cos-policy-profiles roamer_v1 policer-action gbr-bearer
violate-action transmit

```

### Step-by-Step Procedure

To configure a CoS policy profile for roaming subscribers in a 3G network:

1. Specify a name for the CoS policy profile, negotiate the non-GBR traffic class for 3G subscribers, and specify the default to upgrade the traffic class (mapped to QCI value) of create PDP context requests that come in with a lower traffic class than the configured value and downgrade requests with a higher traffic class (numerically lower QCI value).

```

[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
default-bearer-qci 6

```

2. Specify that PDP context requests that come in with a lower ARP (numerically higher) than the configured value are accepted and PDP context requests with a higher ARP (numerically lower) are downgraded to the configured value (default behavior).

```

[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
allocation-retention-priority 5

```



**NOTE:** For GTPv1 subscriber traffic received on the broadband gateway, ARP 1 maps to allocation-retention-priority 1, ARP 2 maps to allocation-retention-priority 6, and ARP 3 maps to allocation-retention-priority 11.



**NOTE:** If the allocation-retention-priority value is not specified, the broadband gateway uses the UE/SGSN requested or negotiated ARP value.

3. Specify that GBR PDP context requests that come in with a lower MBR value than the configured value are accepted, and PDP context requests that come in with a higher MBR values than the configured value are downgraded to the configured MBR value.

```

[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
pdp-qos-control maximum-bit-rate-uplink 2500
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
pdp-qos-control maximum-bit-rate-downlink 2500

```



4. Specify that GBR PDP context requests that come in with a lower GBR value than the configured value are accepted, and PDP context requests that come in with a higher GBR value than the configured value are downgraded to the configured GBR value.

```
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
pdp-qos-control guaranteed-bit-rate-uplink 2372
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
pdp-qos-control guaranteed-bit-rate-downlink 2372
```

5. Configure the uplink and downlink maximum bit rates for traffic classes for non-GBR PDP contexts:

- a. Configure an MBR for the Interactive traffic class with THP 1 (without signaling indication).

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
pdp-qos-control qci 6 maximum-bit-rate-uplink 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
pdp-qos-control qci 6 maximum-bit-rate-downlink 896
```

- b. Configure an MBR for the Interactive traffic class with THP 2.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
pdp-qos-control qci 7 maximum-bit-rate-uplink 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
pdp-qos-control qci 7 maximum-bit-rate-downlink 896
```

- c. Configure an MBR for the Interactive traffic class with THP 3.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
pdp-qos-control qci 8 maximum-bit-rate-uplink 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
pdp-qos-control qci 8 maximum-bit-rate-downlink 896
```

- d. Configure an MBR for the Background traffic class.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
pdp-qos-control qci 9 maximum-bit-rate-uplink 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
pdp-qos-control qci 9 maximum-bit-rate-downlink 896
```

6. Configure the action to take for non-GBR PDP context requests when the MBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
policer-action non-ubr-bearer violate-action transmit
```

7. Configure the action to take for GBR PDP context requests when the GBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
policer-action gbr-bearer exceed-action transmit
```

8. Configure the action to take for GBR PDP context requests when the MBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
policer-action gbr-bearer violate-action transmit
```

**Results** From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

### Configuring a CoS Policy Profile for Roaming Subscribers on a 4G Network

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge cos-cac cos-policy-profiles roamer_v2 default-bearer-qci 6
set unified-edge cos-cac cos-policy-profiles roamer_v2 allocation-retention-priority 5
set unified-edge cos-cac cos-policy-profiles roamer_v2 aggregate-qos-control
maximum-bit-rate-uplink 1600
set unified-edge cos-cac cos-policy-profiles roamer_v2 aggregate-qos-control
maximum-bit-rate-downlink 1600
set unified-edge cos-cac cos-policy-profiles roamer_v2 policer-action non-gbr-bearer
violate-action transmit
```

**Step-by-Step Procedure** To configure a CoS policy profile for roaming subscribers in a 4G network:

1. Specify a name for the CoS policy profile, negotiate the QoS Class Identifier (QCI) for 4G subscribers, and accept bearer requests that come in with a lower QCI (numerically higher) than the configured value and downgrade requests that come in with a higher QCI.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v2
default-bearer-qci 6
```

2. Specify that bearers that come in with a lower ARP (numerically higher) than the configured value are accepted and bearers with a higher ARP (numerically lower) are downgraded to the configured value (default behavior).

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v2
allocation-retention-priority 5
```



**NOTE:** If the allocation-retention-priority value is not specified, the broadband gateway uses the UE/SGW requested or negotiated ARP value.

- Specify that bearers that come in with a lower MBR value than the configured value accepted, and bearers that come in with a higher MBR values than the configured value are downgraded to the configured MBR value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v2
  aggregate-qos-control maximum-bit-rate-uplink 1600
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v2
  aggregate-qos-control maximum-bit-rate-downlink 1600
```

- Configure the action to take for bearers when the AMBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v2
  policer-action non-gbr-bearer violate-action transmit
```

**Results** From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

### Configuring a CoS Policy Profile for Visiting Subscribers on a 3G Network

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge cos-cac cos-policy-profiles visitor_v1 default-bearer-qci 7
set unified-edge cos-cac cos-policy-profiles visitor_v1 allocation-retention-priority 9
set unified-edge cos-cac cos-policy-profiles visitor_v1 pdp-qos-control
  maximum-bit-rate-uplink 2048 upgrade
set unified-edge cos-cac cos-policy-profiles visitor_v1 pdp-qos-control
  maximum-bit-rate-downlink 2048 upgrade
set unified-edge cos-cac cos-policy-profiles visitor_v1 pdp-qos-control
  guaranteed-bit-rate-uplink 1984 upgrade
set unified-edge cos-cac cos-policy-profiles visitor_v1 pdp-qos-control
  guaranteed-bit-rate-downlink 1984 upgrade
set unified-edge cos-cac cos-policy-profiles visitor_v1 pdp-qos-control qci 6
  maximum-bit-rate-uplink 896
set unified-edge cos-cac cos-policy-profiles visitor_v1 pdp-qos-control qci 6
  maximum-bit-rate-downlink 896
set unified-edge cos-cac cos-policy-profiles visitor_v1 pdp-qos-control qci 7
  maximum-bit-rate-uplink 896
set unified-edge cos-cac cos-policy-profiles visitor_v1 pdp-qos-control qci 7
  maximum-bit-rate-downlink 896
set unified-edge cos-cac cos-policy-profiles visitor_v1 pdp-qos-control qci 8
  maximum-bit-rate-uplink 896
set unified-edge cos-cac cos-policy-profiles visitor_v1 pdp-qos-control qci 8
  maximum-bit-rate-downlink 896
set unified-edge cos-cac cos-policy-profiles visitor_v1 pdp-qos-control qci 9
  maximum-bit-rate-uplink 896
set unified-edge cos-cac cos-policy-profiles visitor_v1 pdp-qos-control qci 9
  maximum-bit-rate-downlink 896
```

```

set unified-edge cos-cac cos-policy-profiles visitor_v1 policer-action non-gbr-bearer
violate-action transmit
set unified-edge cos-cac cos-policy-profiles visitor_v1 policer-action gbr-bearer
exceed-action transmit
set unified-edge cos-cac cos-policy-profiles visitor_v1 policer-action gbr-bearer
violate-action transmit

```

### Step-by-Step Procedure

To configure a CoS policy profile for visitor subscribers in a 3G network:

1. Specify a name for the CoS policy profile, negotiate the non-GBR traffic class for 3G subscribers, and specify the default to upgrade the traffic class (mapped to QCI value) of create PDP context requests that come in with a lower traffic class than the configured value and downgrade requests with a higher traffic class (numerically lower QCI value).

```

[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
default-bearer-qci 7

```

2. Specify that PDP context requests that come in with a lower ARP (numerically higher) than the configured value are accepted, and PDP context requests with a higher ARP (numerically lower) are downgraded to the configured value (default behavior).

```

[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
allocation-retention-priority 9

```



**NOTE:** For GTPv1 subscriber traffic received on the broadband gateway, ARP 1 maps to allocation-retention-priority 1, ARP 2 maps to allocation-retention-priority 6, and ARP 3 maps to allocation-retention-priority 11.



**NOTE:** If the allocation-retention-priority value is not specified, the broadband gateway uses the UE/SGSN requested or negotiated ARP value.

3. Specify that GBR PDP context requests that come in with a lower MBR value than the configured value are upgraded to the configured MBR value, and PDP context requests that come in with a higher MBR values than the configured value are downgraded to the configured MBR value.

```

[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
pdp-qos-control maximum-bit-rate-uplink 2048 upgrade
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
pdp-qos-control maximum-bit-rate-downlink 2048 upgrade

```

4. Specify that GBR PDP context requests that come in with a lower GBR value than the configured value are upgraded to the configured GBR value, and PDP context requests that come in with a higher GBR value than the configured value are downgraded to the configured GBR value.

```
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
pdp-qos-control guaranteed-bit-rate-uplink 1984 upgrade
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
pdp-qos-control guaranteed-bit-rate-downlink 1984 upgrade
```

5. Configure the uplink and downlink maximum bit rates for traffic classes for non-GBR PDP contexts:

- a. Configure an MBR for the Interactive traffic class with THP 1 (without signaling indication).

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
pdp-qos-control qci 6 maximum-bit-rate-uplink 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
pdp-qos-control qci 6 maximum-bit-rate-downlink 896
```

- b. Configure an MBR for the Interactive traffic class with THP 2.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
pdp-qos-control qci 7 maximum-bit-rate-uplink 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
pdp-qos-control qci 7 maximum-bit-rate-downlink 896
```

- c. Configure an MBR for the Interactive traffic class with THP 3.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
pdp-qos-control qci 8 maximum-bit-rate-uplink 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
pdp-qos-control qci 8 maximum-bit-rate-downlink 896
```

- d. Configure an MBR for the Background traffic class.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
pdp-qos-control qci 9 maximum-bit-rate-uplink 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
pdp-qos-control qci 9 maximum-bit-rate-downlink 896
```

6. Configure the action to take for non-GBR PDP context requests when the MBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
policer-action non-gbr-bearer violate-action transmit
```

7. Configure the action to take for GBR PDP context requests when the GBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
policer-action gbr-bearer exceed-action transmit
```

8. Configure the action to take for GBR PDP context requests when the MBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
policer-action gbr-bearer violate-action transmit
```

**Results** From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

---

### Configuring a CoS Policy Profile for Visiting Subscribers on a 4G Network

---

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge cos-cac cos-policy-profiles visitor_v2 default-bearer-qci 6 upgrade
set unified-edge cos-cac cos-policy-profiles visitor_v2 allocation-retention-priority 5
upgrade
set unified-edge cos-cac cos-policy-profiles visitor_v2 aggregate-qos-control
maximum-bit-rate-uplink 1600
set unified-edge cos-cac cos-policy-profiles visitor_v2 aggregate-qos-control
maximum-bit-rate-downlink 1600
set unified-edge cos-cac cos-policy-profiles visitor_v2 policer-action non-gbr-bearer
violate-action transmit
```

**Step-by-Step Procedure** To configure a CoS policy profile for visitor subscribers in a 4G network:

1. Specify a name for the CoS policy profile, negotiate the QoS Class Identifier (QCI) for 4G subscribers, and specify the **upgrade** option to upgrade the QCI value of bearer requests that come in with a lower QCI (numerically higher) than the configured value and downgrade requests with a higher QCI.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v2
default-bearer-qci 6 upgrade
```

2. Specify that bearers that come in with a lower ARP (numerically higher) than the configured value are accepted and bearers with a higher ARP (numerically lower) are downgraded to the configured value (default behavior).

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v2
allocation-retention-priority 5
```



---

**NOTE:** If the allocation-retention-priority value is not specified, the broadband gateway uses the UE/SGW requested or negotiated ARP value.

---

- Specify that bearers that come in with a lower MBR value than the configured value are upgraded to the configured MBR value, and bearers that come in with a higher MBR values than the configured value are downgraded to the configured MBR value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v2
aggregate-qos-control maximum-bit-rate-uplink 1600
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v2
aggregate-qos-control maximum-bit-rate-downlink 1600
```

- Configure the action to take for bearers when the AMBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v2
policer-action non-gbr-bearer violate-action transmit
```

**Results** From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

### Configuring a System-Wide CoS Policy Profile

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge cos-cac cos-policy-profiles system_wide default-bearer-qci 6
set unified-edge cos-cac cos-policy-profiles system_wide allocation-retention-priority 5
set unified-edge cos-cac cos-policy-profiles system_wide pdp-qos-control
maximum-bit-rate-uplink 512
set unified-edge cos-cac cos-policy-profiles system_wide pdp-qos-control
maximum-bit-rate-downlink 512
set unified-edge cos-cac cos-policy-profiles system_wide pdp-qos-control
guaranteed-bit-rate-uplink 512
set unified-edge cos-cac cos-policy-profiles system_wide pdp-qos-control
guaranteed-bit-rate-downlink 512
set unified-edge cos-cac cos-policy-profiles system_wide pdp-qos-control qci 6
maximum-bit-rate-uplink 256
set unified-edge cos-cac cos-policy-profiles system_wide pdp-qos-control qci 6
maximum-bit-rate-downlink 256
set unified-edge cos-cac cos-policy-profiles system_wide pdp-qos-control qci 7
maximum-bit-rate-uplink 256
set unified-edge cos-cac cos-policy-profiles system_wide pdp-qos-control qci 7
maximum-bit-rate-downlink 256
set unified-edge cos-cac cos-policy-profiles system_wide pdp-qos-control qci 8
maximum-bit-rate-uplink 256
set unified-edge cos-cac cos-policy-profiles system_wide pdp-qos-control qci 8
maximum-bit-rate-downlink 256
set unified-edge cos-cac cos-policy-profiles system_wide pdp-qos-control qci 9
maximum-bit-rate-uplink 256
set unified-edge cos-cac cos-policy-profiles system_wide pdp-qos-control qci 9
maximum-bit-rate-downlink 256
```

```
set unified-edge cos-cac cos-policy-profiles system_wide aggregate-qos-control
maximum-bit-rate-uplink 256
set unified-edge cos-cac cos-policy-profiles system_wide aggregate-qos-control
maximum-bit-rate-downlink 256
set unified-edge cos-cac cos-policy-profiles system_wide policer-action gbr-bearer
exceed-action transmit
set unified-edge cos-cac cos-policy-profiles system_wide policer-action gbr-bearer
violate-action transmit
set unified-edge cos-cac cos-policy-profiles system_wide policer-action non-gbr-bearer
violate-action transmit
```

**Step-by-Step  
Procedure**

To configure a CoS policy profile for subscribers in 3G and 4G networks:

1. Specify a name for the CoS policy profile, negotiate the QCI for 3G/4G subscribers, and accept bearer requests that come in with a lower traffic class/QCI than the configured value and downgrade requests with a higher traffic class/QCI.

[edit]

```
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
default-bearer-qci 6
```

2. Specify that bearers that come in with a lower ARP (numerically higher) than the configured value are accepted and bearers with a higher ARP (numerically lower) are downgraded to the configured value (the default behavior).

[edit]

```
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
allocation-retention-priority 5
```

3. Specify that PDP context requests that come in with a lower MBR value than the configured value are accepted and PDP context requests that come in with a higher MBR value than the configured value are downgraded to the configured MBR value.

[edit]

```
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
pdp-qos-control maximum-bit-rate-uplink 512
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
pdp-qos-control maximum-bit-rate-downlink 512
```

4. Specify that PDP context requests that come in with a lower GBR value than the configured value are accepted, and PDP context requests that come in with a higher GBR value than the configured value are downgraded to the configured GBR value.

```
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
pdp-qos-control guaranteed-bit-rate-uplink 512
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
pdp-qos-control guaranteed-bit-rate-downlink 512
```



5. Configure the uplink and downlink maximum bit rates for the non-GBR traffic classes:

- a. Configure an MBR for the Interactive traffic class with THP 1 (without signaling indication).

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
pdp-qos-control qci 6 maximum-bit-rate-uplink 256
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
pdp-qos-control qci 6 maximum-bit-rate-downlink 256
```

- b. Configure an MBR for the Interactive traffic class with THP 2.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
pdp-qos-control qci 7 maximum-bit-rate-uplink 256
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
pdp-qos-control qci 7 maximum-bit-rate-downlink 256
```

- c. Configure an MBR for the Interactive traffic class with THP 3.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
pdp-qos-control qci 8 maximum-bit-rate-uplink 256
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
pdp-qos-control qci 8 maximum-bit-rate-downlink 256
```

- d. Configure an MBR for the Background traffic class.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
pdp-qos-control qci 9 maximum-bit-rate-uplink 256
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
pdp-qos-control qci 9 maximum-bit-rate-downlink 256
```

6. Configure the action to take for non-GBR bearer requests when the AMBR or MBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
policer-action non-gbr-bearer violate-action transmit
```

7. Configure the action to take for GBR PDP context requests when the GBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
policer-action gbr-bearer exceed-action transmit
```

8. Configure the action to take for GBR PDP context requests when the MBR exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
policer-action gbr-bearer violate-action transmit
```

**Results** From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

### Configuring Bandwidth Pools

---

**Step-by-Step Procedure** You configure a bandwidth pools for uplink and downlink subscriber traffic to ensure that sufficient bandwidth is available when packet data protocol (PDP) contexts are created or modified. Call admission control (CAC) uses the bandwidth pools to negotiate and reserve bandwidth for PDP contexts with a guaranteed bit rate (GBR).

1. Specify a name for the uplink bandwidth pool.

```
[edit ]
user@host# edit unified-edge cos-cac gbr-bandwidth-pools bw_pool_uplink
```

2. Specify a name for the downlink bandwidth pool.

```
[edit ]
user@host# edit unified-edge cos-cac gbr-bandwidth-pools bw_pool_downlink
```

3. Configure the total bandwidth for each bandwidth pool, in megabits per second (Mbps).

```
[edit]
user@host# set unified-edge cos-cac bandwidth-pools bw_pool_uplink bandwidth
125000
user@host# set unified-edge cos-cac bandwidth-pools bw_pool_downlink bandwidth
500000
```

4. (Optional) Specify that when bearer load reaches the configured bandwidth threshold for uplink or downlink, the create/modify PDP context requests can be downgraded, starting with lower priority requests.

```
[edit]
user@host# set unified-edge cos-cac bandwidth-pools bw_pool_uplink
downgrade-gtp-v1-gbr-bearers
user@host# set unified-edge cos-cac bandwidth-pools bw_pool_downlink
downgrade-gtp-v1-gbr-bearers
```



**NOTE:** If the `downgrade-gtp-v1-gbr-bearers` option is configured and the bandwidth threshold is reached, create or modify PDP context requests arriving on the broadband gateway are downgraded to the Background traffic class. If the `downgrade-gtp-v1-gbr-bearers` option is not configured and the bandwidth threshold is reached, create or modify PDP context requests arriving on the broadband gateway are rejected.

---

### Configuring a Local Policy for 3G Networks

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
edit unified-edge local-policies local_v1
set unified-edge local-policies local_v1 resource-threshold-profile resource_pgw
set unified-edge local-policies local_v1 classifier-profile home_pgw
set unified-edge local-policies local_v1 cos-policy-profile home_v1
set unified-edge local-policies local_v1 roamer-classifier-profile roamer_pgw
set unified-edge local-policies local_v1 roamer-cos-policy-profile roamer_v1
set unified-edge local-policies local_v1 visitor-classifier-profile visitor_pgw
set unified-edge local-policies local_v1 visitor-cos-policy-profile visitor_v1
set unified-edge local-policies local_v1 dl-bandwidth-pool bw_pool_downlink
set unified-edge local-policies local_v1 ul-bandwidth-pool bw_pool_uplink
```

**Step-by-Step Procedure** A local policy defines the QoS treatment to be applied to the broadband gateway at the system level or APN level.

To configure a local policy:

1. Specify a name for the local policy.

```
[edit]
user@ggsn-pgw# edit unified-edge local-policies local_v1
```

2. Specify a resource threshold profile for the local policy to define admission control for managing system overload conditions.

```
[edit]
user@ggsn-pgw# set unified-edge local-policies local_v1 resource-threshold-profile
resource_pgw
```

3. Specify the classifier profiles for the local policy to define the mapping of traffic classes and QCI to a forwarding class and loss priority.

```
[edit]
user@ggsn-pgw# set unified-edge local-policies local_v1 classifier-profile home_pgw
user@ggsn-pgw# set unified-edge local-policies local_v1 roamer-classifier-profile
roamer_pgw
user@ggsn-pgw# set unified-edge local-policies local_v1 visitor-classifier-profile
visitor_pgw
```

4. Specify the CoS policy profiles for the local policy to define the QoS parameters for bearer setup and teardown.

```
[edit]
user@ggsn-pgw# set unified-edge local-policies local_v1 cos-policy-profile home_v1
user@ggsn-pgw# set unified-edge local-policies local_v1 roamer-cos-policy-profile
roamer_v1
user@ggsn-pgw# set unified-edge local-policies local_v1 visitor-cos-policy-profile
visitor_v1
```

5. Specify a bandwidth pool for downlink traffic.

```
[edit]
```

```
user@host# set unified-edge local-policies local_v1 dl-bandwidth-pool  
bw_pool_downlink
```

6. Specify a bandwidth pool for uplink traffic.

```
[edit]  
user@host# set unified-edge local-policies local_v1 ul-bandwidth-pool  
bw_pool_uplink
```

**Results** From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

---

### Configuring a Local Policy for 4G Networks

---

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]  
edit unified-edge local-policies local_v2  
set unified-edge local-policies local_v2 resource-threshold-profile resource_pgw  
set unified-edge local-policies local_v2 classifier-profile home_pgw  
set unified-edge local-policies local_v2 cos-policy-profile home_v2  
set unified-edge local-policies local_v2 roamer-classifier-profile roamer_pgw  
set unified-edge local-policies local_v2 roamer-cos-policy-profile roamer_v2  
set unified-edge local-policies local_v2 visitor-classifier-profile visitor_pgw  
set unified-edge local-policies local_v2 visitor-cos-policy-profile visitor_v2  
set unified-edge local-policies local_v2 dl-bandwidth-pool bw_pool_downlink  
set unified-edge local-policies local_v2 ul-bandwidth-pool bw_pool_uplink
```

**Step-by-Step Procedure** A local policy defines the QoS treatment to be applied to the broadband gateway at the system level or APN level.

To configure a local policy:

1. Specify a name for the local policy.

```
[edit]  
user@ggsn-pgw# edit unified-edge local-policies local_v2
```

2. Specify a resource threshold profile for the local policy to define admission control for managing system overload conditions.

```
[edit]  
user@ggsn-pgw# set unified-edge local-policies local_v2 resource-threshold-profile  
resource_pgw
```

3. Specify the classifier profiles for the local policy to define the mapping of QCI to a forwarding class and loss priority.

```
[edit]  
user@ggsn-pgw# set unified-edge local-policies local_v2 classifier-profile home_pgw  
user@ggsn-pgw# set unified-edge local-policies local_v2 roamer-classifier-profile  
roamer_pgw
```

```
user@ggsn-pgw# set unified-edge local-policies local_v2 visitor-classifier-profile
visitor_pgw
```

4. Specify the CoS policy profiles for the local policy to define the QoS parameters for bearer setup and teardown.

```
[edit]
user@ggsn-pgw# set unified-edge local-policies local_v2 cos-policy-profile home_v2
user@ggsn-pgw# set unified-edge local-policies local_v2 roamer-cos-policy-profile
roamer_v2
user@ggsn-pgw# set unified-edge local-policies local_v2 visitor-cos-policy-profile
visitor_v2
```

5. Specify a bandwidth pool for downlink traffic.

```
[edit ]
user@host# set unified-edge local-policies local_v2 dl-bandwidth-pool
bw_pool_downlink
```

6. Specify a bandwidth pool for uplink traffic.

```
[edit ]
user@host# set unified-edge local-policies local_v2 ul-bandwidth-pool
bw_pool_uplink
```

**Results** From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

### Configuring a System-Wide Local Policy

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
edit unified-edge local-policies local_system_wide
set unified-edge local-policies local_system_wide resource-threshold-profile resource_pgw
set unified-edge local-policies local_system_wide classifier-profile system_wide
set unified-edge local-policies local_system_wide cos-policy-profile system_wide
set unified-edge local-policies local_system_wide dl-bandwidth-pool bw_pool_downlink
set unified-edge local-policies local_system_wide ul-bandwidth-pool bw_pool_uplink
```

**Step-by-Step Procedure** A local policy defines the QoS treatment to be applied to the broadband gateway at the system level or APN level.

To configure a system-wide local policy:

1. Specify a name for the local policy.

```
[edit]
user@ggsn-pgw# edit unified-edge local-policies local_system_wide
```

2. Specify a resource threshold profile for the local policy to define admission control for managing system overload conditions.

```
[edit]
user@ggsn-pgw# set unified-edge local-policies local_system_wide
resource-threshold-profile resource_pgw
```

3. Specify the classifier profile for the local policy to define the mapping of traffic classes and QCI to a forwarding class and loss priority.

```
[edit]
user@ggsn-pgw# set unified-edge local-policies local_system_wide classifier-profile
system_wide
```

4. Specify the CoS policy profiles for the local policy to define the QoS parameters for bearer setup and teardown.

```
[edit]
user@ggsn-pgw# set unified-edge local-policies local_system_wide
cos-policy-profile system_wide
```

5. Specify a bandwidth pool for downlink traffic.

```
[edit ]
user@host# set unified-edge local-policies local_system_wide dl-bandwidth-pool
bw_pool_downlink
```

6. Specify a bandwidth pool for uplink traffic.

```
[edit ]
user@host# set unified-edge local-policies local_system_wide ul-bandwidth-pool
bw_pool_uplink
```

**Results** From configuration mode, confirm your configuration by entering the **show** command at the various hierarchy levels. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

If you are done configuring the device, enter **commit** from configuration mode.

---

### Applying the Local Policies

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set gateways ggsn-pgw MBG1 local-policy-profile local_system_wide
set gateways ggsn-pgw MBG1 apn-services apns qosv1.com local-policy-profile local_v1
set gateways ggsn-pgw MBG1 apn-services apns qosv2.com local-policy-profile local_v2
```

**Step-by-Step Procedure** You apply a local policy at the system level or APN level. A local policy applied at the APN level overrides a local policy at the system level.

1. At the gateway level, apply the system-wide local policy.

```
[edit]
user@host# set gateways ggsn-pgw MBG1 local-policy-profile local_system_wide
```

2. At the APN level, apply the local policy for 3G subscriber traffic.

```
[edit]
```

```
user@host# set gateways ggsn-pgw MBG1 apn-services apns qosv1.com
local-policy-profile local_v1
```

- At the APN level, apply the local policy for 4G subscriber traffic.

```
[edit]
user@host# set gateways ggsn-pgw MBG1 apn-services apns qosv2.com
local-policy-profile local_v2
```

### Configuring DSCP Ingress Rewrite Rules for IPv4 Packets

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
edit class-of-service rewrite-rules dscp dscpv4_ingress_rw]
set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding class af1 loss-priority
high code-point 001110
set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding class af1 loss-priority
low code-point 001010
set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding class af2 loss-priority
high code-point 010110
set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding class af2 loss-priority
low code-point 010010
set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding class af3 loss-priority
high code-point 011110
set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding class af3 loss-priority
low code-point 011010
set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding class af4 loss-priority
high code-point 100110
set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding class af4 loss-priority
low code-point 100010
```

#### Step-by-Step Procedure

To configure the ingress rewrite rules for IPv4 packets:

- Specify a name for the ingress rewrite rules.

```
[edit]
user@host# edit class-of-service rewrite-rules dscp dscpv4_ingress_rw
```

- Configure the ingress rewrite rules mappings for traffic on the mobile interface.

```
[edit]
user@host# set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding
class af1 loss-priority high code-point 001110
user@host# set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding
class af1 loss-priority low code-point 001010
user@host# set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding
class af2 loss-priority high code-point 010110
user@host# set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding
class af2 loss-priority low code-point 010010
user@host# set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding
class af3 loss-priority high code-point 011110
user@host# set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding
class af3 loss-priority low code-point 011010
user@host# set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding
class af4 loss-priority high code-point 100110
```

```
user@host# set class-of-service rewrite-rules dscp dscpipv4_ingress_rw forwarding
class af4 loss-priority low code-point 100010
```

### Configuring DSCP Ingress Rewrite Rules for IPv6 Packets

---

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
edit class-of-service rewrite-rules dscp dscpipv6_ingress_rw
set class-of-service rewrite-rules dscp dscpipv6_ingress_rw forwarding class af1 loss-priority
high code-point 001110
set class-of-service rewrite-rules dscp dscpipv6_ingress_rw forwarding class af1 loss-priority
low code-point 001010
set class-of-service rewrite-rules dscp dscpipv6_ingress_rw forwarding class af2 loss-priority
high code-point 010110
set class-of-service rewrite-rules dscp dscpipv6_ingress_rw forwarding class af2 loss-priority
low code-point 010010
set class-of-service rewrite-rules dscp dscpipv6_ingress_rw forwarding class af3 loss-priority
high code-point 011110
set class-of-service rewrite-rules dscp dscpipv6_ingress_rw forwarding class af3 loss-priority
low code-point 011010
set class-of-service rewrite-rules dscp dscpipv6_ingress_rw forwarding class af4 loss-priority
high code-point 100110
set class-of-service rewrite-rules dscp dscpipv6_ingress_rw forwarding class af4 loss-priority
low code-point 100010
```

#### Step-by-Step Procedure

To configure the ingress rewrite rules for IPv6 packets:

1. Specify a name for the ingress rewrite rules.

```
[edit]
user@host# edit class-of-service rewrite-rules dscp-ipv6 dscpipv6_ingress_rw
```

2. Configure the ingress rewrite rules mappings for traffic on the mobile interface.

```
[edit]
user@host# set class-of-service rewrite-rules dscp dscpipv6_ingress_rw forwarding
class af1 loss-priority high code-point 001110
user@host# set class-of-service rewrite-rules dscp dscpipv6_ingress_rw forwarding
class af1 loss-priority low code-point 001010
user@host# set class-of-service rewrite-rules dscp dscpipv6_ingress_rw forwarding
class af2 loss-priority high code-point 010110
user@host# set class-of-service rewrite-rules dscp dscpipv6_ingress_rw forwarding
class af2 loss-priority low code-point 010010
user@host# set class-of-service rewrite-rules dscp dscpipv6_ingress_rw forwarding
class af3 loss-priority high code-point 011110
user@host# set class-of-service rewrite-rules dscp dscpipv6_ingress_rw forwarding
class af3 loss-priority low code-point 011010
user@host# set class-of-service rewrite-rules dscp dscpipv6_ingress_rw forwarding
class af4 loss-priority high code-point 100110
user@host# set class-of-service rewrite-rules dscp dscpipv6_ingress_rw forwarding
class af4 loss-priority low code-point 100010
```



### Configuring DSCP Egress Rewrite Rules for IPv4 Packets

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
edit class-of-service rewrite-rules dscp dscp_v4_egress_rw
set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding class af1 loss-priority
  high code-point 001110
set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding class af1 loss-priority
  low code-point 001010
set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding class af2 loss-priority
  high code-point 010110
set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding class af2 loss-priority
  low code-point 010010
set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding class af3 loss-priority
  high code-point 011110
set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding class af3 loss-priority
  low code-point 011010
set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding class af4 loss-priority
  high code-point 100110
set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding class af4 loss-priority
  low code-point 100010
set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding class be loss-priority
  low code-point 000000
```

**Step-by-Step Procedure** To configure the egress rewrite rules for IPv4 packets:

1. Specify a name for the egress rewrite rules.

```
[edit ]
user@host# edit class-of-service rewrite-rules dscp dscp_v4_egress_rw
```

2. Configure the egress rewrite rules mappings for traffic on the mobile interface.

```
[edit]
user@host# set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding
  class af1 loss-priority high code-point 001110
user@host# set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding
  class af1 loss-priority low code-point 001010
user@host# set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding
  class af2 loss-priority high code-point 010110
user@host# set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding
  class af2 loss-priority low code-point 010010
user@host# set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding
  class af3 loss-priority high code-point 011110
user@host# set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding
  class af3 loss-priority low code-point 011010
user@host# set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding
  class af4 loss-priority high code-point 100110
user@host# set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding
  class af4 loss-priority low code-point 100010
user@host# set class-of-service rewrite-rules dscp dscp_v4_egress_rw forwarding
  class be loss-priority low code-point 000000
```

## Configuring DSCP Egress Rewrite Rules for IPv6 Packets

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
edit class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw
set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw forwarding class af1
  loss-priority high code-point 001110
set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw forwarding class af1
  loss-priority low code-point 001010
set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw forwarding class af2
  loss-priority high code-point 010110
set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw forwarding class af2
  loss-priority low code-point 010010
set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw forwarding class af3
  loss-priority high code-point 011110
set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw forwarding class af3
  loss-priority low code-point 011010
set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw forwarding class af4
  loss-priority high code-point 100110
set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw forwarding class af4
  loss-priority low code-point 100010
set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw forwarding class be
  loss-priority low code-point 000000
```

**Step-by-Step Procedure** To configure the ingress rewrite rules for IPv6 packets:

1. Specify a name for the egress rewrite rules.
2. Configure the egress rewrite rules mappings for traffic on the mobile interface.

```
[edit]
user@host# edit class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw
  forwarding class af1 loss-priority high code-point 001110
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw
  forwarding class af1 loss-priority low code-point 001010
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw
  forwarding class af2 loss-priority high code-point 010110
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw
  forwarding class af2 loss-priority low code-point 010010
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw
  forwarding class af3 loss-priority high code-point 011110
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw
  forwarding class af3 loss-priority low code-point 011010
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw
  forwarding class af4 loss-priority high code-point 100110
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw
  forwarding class af4 loss-priority low code-point 100010
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpv6_egress_rw
  forwarding class be loss-priority low code-point 000000
```

### Applying Ingress Rewrite Rules to Mobile Interfaces for 3G and 4G Subscriber Traffic

- CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:
- ```
[edit]
set class-of-service interfaces mif unit 0 ingress-rewrite-rules dscp dscp4_ingress_rw
set class-of-service interfaces mif unit 0 ingress-rewrite-rules dscp-ipv6 dscp6_ingress_rw
set class-of-service interfaces mif unit 1 ingress-rewrite-rules dscp dscp4_ingress_rw
set class-of-service interfaces mif unit 1 ingress-rewrite-rules dscp-ipv6 dscp6_ingress_rw
```
- Step-by-Step Procedure** To specify the ingress rewrite rules to apply to rewrite DSCPv4 and DSCPv6 values for incoming subscriber packets on the mif.0 and mif.1 mobile interfaces, which correspond to the **qosv1.com** and **qosv2.com** APNs for 3G subscriber traffic and 4G subscriber traffic, respectively:
1. To apply ingress rewrite rules to change DSCPv4 and DSCPv6 values in the outer IP header of 3G subscriber packets arriving on the **qosv1.com** APN (mif.0), specify the names of the rewrite rules that you want to apply to the mobile interface.
 

```
[edit]
user@host# set class-of-service interfaces mif unit 0 ingress-rewrite-rules dscp
dscp4_ingress_rw
user@host# set class-of-service interfaces mif unit 0 ingress-rewrite-rules dscp-ipv6
dscp6_ingress_rw
```
  2. To apply ingress rewrite rules to change DSCPv4 and DSCPv6 values in the outer IP header of 4G subscriber packets arriving on the **qosv2.com** APN (mif.1), specify the names of the rewrite rules that you want to apply to the mobile interface.
 

```
[edit]
user@host# set class-of-service interfaces mif unit 1 ingress-rewrite-rules dscp
dscp4_ingress_rw
user@host# set class-of-service interfaces mif unit 1 ingress-rewrite-rules dscp-ipv6
dscp6_ingress_rw
```

### Applying Egress Rewrite Rules to Mobile Interfaces for 3G and 4G Subscriber Traffic

- CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:
- ```
[edit]
set class-of-service interfaces mif unit 0 rewrite-rules dscp dscp4_egress_rw protocol
gtp-inet-both
set class-of-service interfaces mif unit 0 rewrite-rules dscp dscp6_egress_rw protocol
gtp-inet-both
set class-of-service interfaces mif unit 1 rewrite-rules dscp dscp4_egress_rw protocol
gtp-inet-both
set class-of-service interfaces mif unit 1 rewrite-rules dscp dscp6_egress_rw protocol
gtp-inet-both
```

**Step-by-Step Procedure** To apply an egress rewrite rule to rewrite DSCPv4 and DSCPv6 values to both the inner and outer IP headers of downstream subscriber packets, specify the name of the rewrite rules you want to apply to the mobile interfaces and include the **gtp-inet-both** option:

1. To apply egress rewrite rules to change DSCPv4 and DSCPv6 values in the outer IP header of 3G subscriber packets arriving on the **qosv1.com** APN (mif.0), specify the names of the rewrite rules that you want to apply to the mobile interface.

```
[edit]
user@host# set class-of-service interfaces mif unit 0 rewrite-rules dscp
dscp4_egress_rw protocol gtp-inet-both
user@host# set class-of-service interfaces mif unit 0 rewrite-rules dscp
dscp6_egress_rw protocol gtp-inet-both
```

```
[edit]
user@host# set class-of-service interfaces mif unit 1 rewrite-rules dscp
dscp4_egress_rw protocol gtp-inet-both
user@host# set class-of-service interfaces mif unit 1 rewrite-rules dscp
dscp6_egress_rw protocol gtp-inet-both
```

2. To apply ingress rewrite rules to change DSCPv4 and DSCPv6 values in the outer IP header of 4G subscriber packets arriving on the **qosv2.com** APN (mif.1), specify the names of the rewrite rules that you want to apply to the mobile interface.

```
[edit]
user@host# set class-of-service interfaces mif unit 1 rewrite-rules dscp
dscp4_egress_rw protocol gtp-inet-both
user@host# set class-of-service interfaces mif unit 1 rewrite-rules dscp
dscp6_egress_rw protocol gtp-inet-both
```

### Configuring the Maximum Number of Bearers

---

**Step-by-Step Procedure** You configure the maximum bearers to specify an upper limit on the number of bearers allowed at the system level and, optionally, the APN level. When the total number of active bearers at the system level or APN level reaches the maximum configured limit, the broadband gateway rejects new bearer requests.

To configure the maximum number of active bearers:

1. Configure the number of maximum bearers allowed at the system level.

```
[edit]
user@host# set unified-edge gateways ggsn-pgw MBG1 maximum-bearers 5000000
```

### Enabling Preemption

---

**Step-by-Step Procedure** You can enable preemption at the system level to enable the preemption capability indicator (PCI) and preemption vulnerability indicator (PVI) flags. Preemption is disabled by default.

To enable preemption or both 3G (GTPv1) and 4G (GTPv2) subscriber traffic:

1. Configure preemption at the system level.

```
[edit]
```

```
user@host# set unified-edge gateways ggsn-pgw MBG1 preemption enable
```

## Verification

To display QoS statistics for 3G and 4G subscriber packets to verify that the QoS configuration on the broadband gateway is working properly, you can perform the following tasks:

- [Display QoS Statistics for 4G Subscriber Packets with a Specified Allocation Retention Priority: on page 575](#)
- [Display 4G Subscriber Information for Traffic Marked with a Specified QCI on page 576](#)
- [Display 3G Subscriber Information for Traffic Marked with the Specified Traffic Class on page 577](#)
- [Display the Requested and Negotiated QoS Parameters for Mobile Subscribers on page 578](#)

### Display QoS Statistics for 4G Subscriber Packets with a Specified Allocation Retention Priority:

---

**Purpose** Verify that the QoS configuration is working properly by displaying statistics such as session establishment attempts, peer initiated sessions, and gateway initiated session deactivations.

**Action** user@host> show unified-edge ggsn-pgw statistics arp 10

```
Control plane statistics:
  Gn/S5 signaling msgs rcvd:          0
  Gn/S5 signaling msgs sent:         50001
  Gn/S5 signaling msgs dropped:       0
  Gn/S5 signaling bytes rcvd:         0
  Gn/S5 signaling bytes sent:         0
  Total GTP tunnels created:          0
  Session establishment attempts:     50221
  Successful session establishments:   4476
  MS/peer initiated session deactivations: 0
  Successful MS/peer initiated deactivations: 0
  Gateway initiated session deactivations: 0
  Successful gateway initiated deactivations: 0
  Session Establishments Failed (by GTP cause):
    Others: 0
    Service unavailable: 0
    System failure: 0
    No resources: 47762
    No address: 0
    Service denied: 0
    Authentication Fail: 0
    APN access denied: 0
  Data plane GTP statistics (Gn/S5/S8):
    Input packets: 0
    Input bytes: 0
    Output packets: 0
    Output bytes: 0
    Discarded packets: 0
  Data plane GTP statistics (Gi):
    Input packets: 0
    Input bytes: 0
    Output packets: 0
    Output bytes: 0
    Discarded packets: 0
```

**Meaning** This output shows the attempted session requests and the requests that were successfully established for 4G subscriber traffic with the specified ARP value.

#### Display 4G Subscriber Information for Traffic Marked with a Specified QCI

**Purpose** Verify that the QoS configuration is working properly for 4G subscribers by showing statistics for subscriber packets with a specified QCI.

**Action** user@host> show unified-edge ggsn-pgw statistics qci 5  
 regress@brainstorm> show unified-edge ggsn-pgw qos statistics qci 5

Control plane statistics:

|                                               |    |
|-----------------------------------------------|----|
| Gn/S5 signaling msgs rcvd:                    | 0  |
| Gn/S5 signaling msgs sent:                    | 10 |
| Gn/S5 signaling msgs dropped:                 | 0  |
| Gn/S5 signaling bytes rcvd:                   | 0  |
| Gn/S5 signaling bytes sent:                   | 0  |
| Total GTP tunnels created:                    | 0  |
| Session establishment attempts:               | 10 |
| Successful session establishments:            | 10 |
| MS/peer initiated session deactivations:      | 0  |
| Successful MS/peer initiated deactivations:   | 0  |
| Gateway initiated session deactivations:      | 0  |
| Successful gateway initiated deactivations:   | 0  |
| Session Establishments Failed (by GTP cause): |    |
| Others                                        | 0  |
| Service unavailable:                          | 0  |
| System failure:                               | 0  |
| No resources:                                 | 0  |
| No address:                                   | 0  |
| Service denied:                               | 0  |
| Authentication Fail:                          | 0  |
| APN access denied:                            | 0  |

**Meaning** This output shows the Create Session requests that were successfully established for 4G mobile subscriber packets with the specified QCI value.

### Display 3G Subscriber Information for Traffic Marked with the Specified Traffic Class

**Purpose** Verify that the QoS configuration is working properly for 3G subscribers by showing statistics for subscriber packets of the specified traffic class.

**Action** user@host> show unified-edge ggsn-pgw statistics traffic-class conversational

```
Control plane statistics:
Gn/S5 signaling msgs rcvd:          0
Gn/S5 signaling msgs sent:         15
Gn/S5 signaling msgs dropped:       0
Gn/S5 signaling bytes rcvd:         0
Gn/S5 signaling bytes sent:         0
Total GTP tunnels created:          0
Session establishment attempts:     15
Successful session establishments:   15
MS/peer initiated session deactivations: 0
Successful MS/peer initiated deactivations: 0
Gateway initiated session deactivations: 0
Successful gateway initiated deactivations: 0
Session Establishments Failed (by GTP cause):
  Others: 0
  Service unavailable: 0
  System failure: 0
  No resources: 0
  No address: 0
  Service denied: 0
  Authentication Fail: 0
  APN access denied: 0
Data plane GTP statistics (Gn/S5/S8):
  Input packets: 0
  Input bytes: 0
  Output packets: 0
  Output bytes: 0
  Discarded packets: 0
Data plane GTP statistics (Gi):
  Input packets: 0
  Input bytes: 0
  Output packets: 0
  Output bytes: 0
  Discarded packets: 0
```

**Meaning** This output shows the Create Session requests that were successfully established for 3G subscriber traffic of the conversational class.

#### [Display the Requested and Negotiated QoS Parameters for Mobile Subscribers](#)

**Purpose** Verify the negotiated QoS parameters for a mobile subscriber.



```

Action user@host> show unified-edge ggsn-pgw subscribers extensive
Subscriber Information:
  IMSI: 332215553443196   IMEI: 1122334455667795
  MSISDN: 3326555562     Time Zone: None   (DST): None
  Status: Visitor
User Location Info:
  MCC: None MNC: None
  LAC: 0x0 CI: 0x0 SAC: 0x0 RAC: 0x0 TAC: 0x0 ECI: 0x0
  RAT Type: E-UTRAN
PDN Session:
  APN name: juniper.com
  IPv4 Address: 20.0.4.8   IPv6 Address: None
  Direct Tunnel: Disabled   Session Duration: 3d 20:38:38
  Local Control address: 10.1.1.1 Remote Control address: 30.1.1.2
  TEID Control Local: 0x9001800 TEID Control Remote: 0x10d
  Peer CSID: 0             Remote CSID: 0
  Addressing scheme: Local   Selection mode: from-ms
  Session PIC: 0 /0 (FPC/PIC) Anchor PFE: 2 /0 (FPC/PIC)
  Session State: Established GTP Version: 2
  Serving network: MCC: 231 MNC :215
  Negotiated APN AMBR: Downlink: 1000 kbps   Uplink: 1000 kbps
  Requested APN AMBR: Downlink: 1000 kbps   Uplink: 1000 kbps
Bearer:
  NSAPI/EBI: 5             Charging ID: 0x9001800
  Local Data address: 10.1.1.1 Remote Data address: 30.1.1.2
  Local TEID: 0x111000     Remote TEID: 0x10e
  Bearer State: Established Substate: -
  Idle Timeout: 0 min(0 -0,0) AAA Interim Interval: 0 min(0 -0,0)
Negotiated QoS Parameters:
  QCI: 5 ARP: 11/0 /0 (PL/PVI/PCI)
  Forwarding Class: -       Loss Priority: -
Requested QoS Parameters:
  QCI :5 ARP : 11/0 /0 (PL/PVI/PCI)
Charging information:
  Profile ID: 0
  State: Init               Previous State: Init

```

**Meaning** This output shows the negotiated and requested QoS parameters for mobile subscribers.

- Related Documentation**
- [Quality of Service Overview on page 499](#)
  - [Call Admission Control Overview on page 506](#)
  - [Class of Service \(CoS\) Policy Profile Overview on page 508](#)
  - [Policing Subscriber Traffic on the Broadband Gateway Overview on page 509](#)
  - [Configuring QoS on the Broadband Gateway Overview on page 516](#)
  - [Configuring S-GW-Specific CAC Parameters on page 581](#)
  - [Example: Configuring QoS and CAC on a S-GW on page 582](#)

## Verifying Quality of Service

**Purpose** Display QoS statistics for subscriber packets.

- Action**
- To display QoS statistics information for the specified gateway:

```
user@host> show unified-edge ggsn-pgw statistics gateway
```

- To display subscriber information for traffic marked with the specified GTPv1 allocation retention priority:

```
user@host> show unified-edge ggsn-pgw statistics gtpv1-arp arp-value
```



**NOTE:** You can specify an ARP value of 1 through 3.

- To display subscriber information for traffic marked with the specified GTPv2 allocation retention priority:

```
user@host> show unified-edge ggsn-pgw statistics gtpv2-priority-level arp-value
```



**NOTE:** You can specify an ARP value of 1 through 15.

- To display subscriber information for traffic marked with the specified GTPv1 allocation retention priority:

```
user@host> show unified-edge ggsn-pgw statistics gtpv1-arp
```

- To display subscriber information for traffic marked with the specified QoS Class Identifier:

```
user@host> show unified-edge ggsn-pgw statistics qci qci-value
```



**NOTE:** You can specify a QCI value of 1 through 9.

- To display subscriber information for traffic marked with the specified traffic class:

```
user@host> show unified-edge ggsn-pgw statistics traffic-class (background |
conversational | interactive | streaming)
```

- To display the status information for the interactive traffic class with a specified traffic handling priority:

```
show unified-edge ggsn-pgw statistics traffic-class interactive
traffic-handling-priority traffic-handling-priority
```



**NOTE:** You can specify a traffic-handling priority value of 1 through 3.

#### Related Documentation

- [Configuring a Classifier Profile for 3G and 4G Networks on page 521](#)
- [Configuring a CoS Policy Profile for 3G and 4G Networks on page 531](#)
- [Configuring QoS on the Broadband Gateway Overview on page 516](#)

## Configuring S-GW-Specific CAC Parameters

The MobileNext Broadband Gateway Serving Gateway (S-GW) uses three statements unique to the S-GW for connection admission control (CAC). This topic shows how to configure the CAC statements that are unique to the S-GW.

Before you begin configuring a S-GW CAC parameters on the broadband gateway, you should have done the following:

- Configured the chassis of the MobileNext Broadband Gateway
- Configured the interfaces used by the MobileNext Broadband Gateway

To establish the CAC parameters unique to the S-GW, you can establish values for the default bearers as a percentage of anchor PFEs, the guaranteed bandwidth of the anchor PFEs, and maximum number of bearers for the anchor PFE. The use of all three statements is optional and all have default values.

To configure the S-GW CAC parameters:

1. Optionally, configure the S-GW anchor PFE default bearer percentage.

```
[edit unified-edge gateways sgw MBG-SGW1]
user@host# set anchor-pfe-default-bearers-percentage 50
```



**NOTE:** You can use any value from 10 through 100 percent.

2. Optionally, configure the S-GW anchor PFE guaranteed bandwidth.

```
[edit unified-edge gateways sgw MBG-SGW1]
user@host# set anchor-pfe-guaranteed-bandwidth 10
```



**NOTE:** You can use any value from 10 through 100 Gigibits per second.

3. Optionally, configure the S-GW anchor PFE maximum bearers.

```
[edit unified-edge gateways sgw MBG-SGW1]
user@host# set anchor-pfe-maximum-bearers 200
```



**NOTE:** You can use any value from 100 through 512 thousand bearers.

### Related Documentation

- [Quality of Service Overview on page 499](#)
- [Call Admission Control Overview on page 506](#)
- [Example: Configuring QoS and CAC on a S-GW on page 582](#)

## Example: Configuring QoS and CAC on a S-GW

---

This example describes how to configure the MobileNext Broadband Gateway Serving Gateway (S-GW) for quality of service (QoS) and connection access control (CAC). The emphasis is on QoS and CAC configuration, and does not include many other parameters that a full S-GW configuration requires.

The example configures classifiers and resource thresholds for the S-GW for forwarding classes af1 and af3, setting thresholds for bearer loads, memory, and CPU usage. Preemption is enabled for the S-GW. Rewrite rules are also configured for ingress and egress traffic, setting DSCP bits for high and low loss priority for classes af1 and af3. The classifier and threshold profiles, as well as the rewrite rules, are applied to a S-GW with anchor Packet Forwarding Engine CAC parameters, specifically the S5 and S11 interfaces.

- [Requirements on page 582](#)
- [Overview on page 582](#)
- [Configuration on page 582](#)

### Requirements

This example uses the following hardware and software components:

- Junos OS Release 11.4W
- Juniper Networks MobileNext Broadband Gateway

### Overview

This example describes how to configure the broadband gateway as a standalone S-GW (SGW-MBG1) with QoS and CAC parameters. The S-GW supports the following configuration:

- The S5 and S11 interfaces are in the main routing instance and use **xe-0/0/0** and **ge-5/0/2**, respectively.
- All eight queues are enabled, but only forwarding classes af1 and af3 have classifiers and rewrite rules for transport traffic.
- Rewrite rules for af1 and af3 are applied for ingress traffic on the S5 interface (**xe-0/0/0**) and egress traffic on the S11 interface (**ge-5/0/2**).



**NOTE:** This is not a complete S-GW configuration. This example illustrates QoS and CAC only.

---

### Configuration

- [Configuring the interfaces on page 583](#)
- [Configuring the IPv4 Interfaces on page 583](#)

- [Configuring the QoS and CAC Classifier and Resource Threshold Profiles and Parameters on page 584](#)
- [Configuring S-GW CAC Parameters on page 585](#)
- [Configuring Forwarding Classes and Rewrite Rules on page 586](#)
- [Apply the Rewrite Rule for Ingress \(S5\) and Egress \(S11\) on page 586](#)

### Configuring the interfaces

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set interface xe-0/0/0 description S5 interface
set interface xe-0/0/0 unit 0 family inet address 10.1.1.1/24
set interface ge-5/0/2 description S11 interface
set interface ge-5/0/2 unit 0 family inet address 172.16.1.1/24
```

**Step-by-Step Procedure** To configure the IPv4 interfaces:

1. Configure the S5 interface.
 

```
[edit interfaces]
user@sgw1# set xe-0/0/0 description S5 interface
user@sgw1# set xe-0/0/0 unit 0 family inet address 10.1.1.1/24
```
2. Configure the S11 interface.
 

```
[edit interfaces]
user@sgw1# set ge-5/0/2 description S11 interface
user@sgw1# set ge-5/0/2 unit 0 family inet address 172.16.1.1/24
```

### Configuring the IPv4 Interfaces

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set interfaces ge-0/0/0 unit 0 family inet address 10.44.0.1/16 description S5 interface
set interfaces ge-0/0/1 unit 0 family inet address 10.2.2.1/16 description S11 interface
```

**Step-by-Step Procedure** To configure the IPv4 interfaces:

1. Configure IPv4 interfaces for the S5 interface.
 

```
[edit]
user@sgw1# set interfaces ge-0/0/0 unit 0 family inet address 10.44.0.1/16
```
2. Configure IPv4 interfaces for the S11 interface.
 

```
[edit]
user@sgw1# set interfaces ge-0/0/1 unit 0 family inet address 10.2.2.1/16
```

## Configuring the QoS and CAC Classifier and Resource Threshold Profiles and Parameters

---

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CLI Quick Configuration</b> | <p>To quickly configure this example, copy the following commands and paste them into the router terminal window:</p> <pre>[edit] set unified-edge cos-cac classifier-profiles classifier_v2 set unified-edge cos-cac classifier-profiles classifier_v2 qos-class-identifier 6   forwarding-class af1 loss-priority low set unified-edge cos-cac classifier-profiles classifier_v2 qos-class-identifier 3   forwarding-class af3 loss-priority high set unified-edge cos-cac resources-threshold-profiles resource_v2 set unified-edge cos-cac resources-threshold-profiles resource_v2 bearers-load low   percentage 70 set unified-edge cos-cac resources-threshold-profiles resource_v2 bearers-load low   gtpv2-priority-level 9 set unified-edge cos-cac resources-threshold-profiles resource_v2 bearers-load high   percentage 90 set unified-edge cos-cac resources-threshold-profiles resource_v2 bearers-load high   gtpv2-priority-level 5 set unified-edge cos-cac resources-threshold-profiles resource_v2 memory low percentage   60 set unified-edge cos-cac resources-threshold-profiles resource_v2 memory low   gtpv2-priority-level 8 set unified-edge cos-cac resources-threshold-profiles resource_v2 memory high percentage   70 set unified-edge cos-cac resources-threshold-profiles resource_v2 memory high   gtpv2-priority-level 4 set unified-edge cos-cac resources-threshold-profiles resource_v2 cpu low percentage 65 set unified-edge cos-cac resources-threshold-profiles resource_v2 cpu low   gtpv2-priority-level 10 set unified-edge cos-cac resources-threshold-profiles resource_v2cpu high percentage   80 set unified-edge cos-cac resources-threshold-profiles resource_v2 cpu high   gtpv2-priority-level 7 set unified-edge local-policies local_profile_v2 resource-threshold-profiles resource_v2 set unified-edge local-policies local_profile_v2 classifier-profiles classifier_v2</pre> |
| <b>Step-by-Step Procedure</b>  | <p>To configure the QoS and CAC classifier and resource threshold profiles and parameters:</p> <ol style="list-style-type: none"><li>1. Configure classifier profile <b>classifier_v2</b>.<br/><pre>[edit] user@sgw1# edit unified-edge cos-cac classifier-profiles classifier_v2</pre></li><li>2. Specify the QoS parameters for af1 and af3.<br/><pre>[edit unified-edge cos-cac classifier-profiles classifier_v2] user@sgw1# set qos-class-identifier 6 forwarding-class af1 loss-priority low user@sgw1# set qos-class-identifier 3 forwarding-class af3 loss-priority high</pre></li><li>3. Configure resource threshold profile <b>resource_v2</b>.<br/><pre>[edit] user@sgw1# edit unified-edge cos-cac resource-threshold-profiles resource_v2</pre></li></ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

- Specify the resource threshold parameters for bearer load, memory, and CPU.

```
[edit unified-edge cos-cac resource-threshold-profiles resource_v2]
user@sgw1# set bearers-load low percentage 70
user@sgw1# set bearers-load low gtpv2-priority-level 9
user@sgw1# set bearers-load high percentage 90
user@sgw1# set bearers-load high gtpv2-priority-level 5
user@sgw1# set memory low percentage 60
user@sgw1# set memory low gtpv2-priority-level 8
user@sgw1# set memory high percentage 70
user@sgw1# set memory high gtpv2-priority-level 4
user@sgw1# set cpu low percentage 65
user@sgw1# set cpu low gtpv2-priority-level 10
user@sgw1# set cpu high percentage 80
user@sgw1# set cpu high gtpv2-priority-level 7
```

- Configure the local policy `local_profile_v2`.

```
[edit]
user@sgw1# edit unified-edge local-policies local_profile_v2
```

- Configure the local policies for the classifier and resource threshold profiles.

```
[edit unified-edge local-policies local_profile_v2]
user@sgw1# set resource-threshold-profile resource_v2
user@sgw1# set classifier-profile classifier_v2
```

### Configuring S-GW CAC Parameters

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge gateways sgw SGW-MBG1 maximum-bearers 100000
set unified-edge gateways sgw SGW-MBG1 local-policy-profile local_profile_v2
set unified-edge gateways sgw SGW-MBG1 anchor-pfe-guaranteed-bandwidth 10 # Gbps
set unified-edge gateways sgw SGW-MBG1 anchor-pfe-maximum-bearers 100 # thousands
set unified-edge gateways sgw SGW-MBG1 anchor-pfe-guaranteed-bandwidth 10 # Gbps
set unified-edge gateways sgw SGW-MBG1 anchor-pfe-default-bearers-percentage 60
set unified-edge gateways sgw SGW-MBG1 preemption enable
```

#### Step-by-Step Procedure

To configure the S-GW CAC parameters:

- Configure the maximum bearers and local policy profile.

```
[edit unified-edge gateways sgw SGW-MBG1]
user@sgw1# set maximum-bearers 100000
user@sgw1# set local-policy-profile local_profile_v2
```

- Configure the anchor CAC parameters.

```
[edit unified-edge gateways sgw SGW-MBG1]
user@sgw1# set anchor-pfe-guaranteed-bandwidth 10 # Gbps
user@sgw1# set anchor-pfe-maximum-bearers 100 # thousands
user@sgw1# set anchor-pfe-default-bearers-percentage 60
user@sgw1# set preemption enable
```

### Configuring Forwarding Classes and Rewrite Rules

---

- CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:
- ```
[edit]
set class-of-service forwarding-classes queue 0 be
set class-of-service forwarding-classes queue 1 ef
set class-of-service forwarding-classes queue 2 af1
set class-of-service forwarding-classes queue 3 af2
set class-of-service forwarding-classes queue 4 af3
set class-of-service forwarding-classes queue 5 af4
set class-of-service forwarding-classes queue 6 af5
set class-of-service forwarding-classes queue 7 nc
set class-of-service rewrite-rules dscp dscp_egress forwarding-class af1 loss-priority low
  code-point 001010
set class-of-service rewrite-rules dscp dscp_egress forwarding-class af3 loss-priority high
  code-point 011110
set class-of-service rewrite-rules dscp dscp_ingress forwarding-class af1 loss-priority low
  code-point 001010
set class-of-service rewrite-rules dscp dscp_ingress forwarding-class af3 loss-priority high
  code-point 011110
```
- Step-by-Step Procedure** To configure forwarding classes and rewrite rules:
1. Configure the forwarding classes.  

```
[edit class-of-service]
user@sgw1# set forwarding-classes queue 0 be
user@sgw1# set forwarding-classes queue 1 ef
user@sgw1# set forwarding-classes queue 2 af1
user@sgw1# set forwarding-classes queue 3 af2
user@sgw1# set forwarding-classes queue 4 af3
user@sgw1# set forwarding-classes queue 5 af4
user@sgw1# set forwarding-classes queue 6 af5
user@sgw1# set forwarding-classes queue 7 nc
```
  2. Configure the rewrite rules.  

```
[edit class-of-service]
user@sgw1# set rewrite-rules dscp dscp_egress forwarding-class af1 loss-priority
  low code-point 001010
user@sgw1# set rewrite-rules dscp dscp_egress forwarding-class af3 loss-priority
  high code-point 011110
user@sgw1# set rewrite-rules dscp dscp_ingress forwarding-class af1 loss-priority
  low code-point 001010
user@sgw1# set rewrite-rules dscp dscp_ingress forwarding-class af3 loss-priority
  high code-point 011110
```

### Apply the Rewrite Rule for Ingress (S5) and Egress (S11)

---

- CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
```



```
set class-of-service interfaces xe-0/0/0 unit 0 rewrite-rules dscp dcsp_ingress
set class-of-service interfaces ge-5/0/2 unit 0 rewrite-rules dscp dcsp_egress
```

**Step-by-Step  
Procedure**

To configure the rewrite rules on the S5 and S11 interfaces:

1. Configure the ingress rewrite rule on the S5 interface.  

```
[edit class-of-service]
user@sgw1# set interfaces xe-0/0/0 unit 0 rewrite-rules dscp dcsp_ingress
```
2. Configure the egress rewrite rule on the S11 interface.  

```
[edit class-of-service]
user@sgw1# set interfaces ge-5/0/2 unit 0 rewrite-rules dscp dcsp_egress
```

**Related  
Documentation**

- [Quality of Service Overview on page 499](#)
- [Call Admission Control Overview on page 506](#)
- [Configuring S-GW-Specific CAC Parameters on page 581](#)



## PART 10

# Maintenance

- [Maintenance Mode on page 591](#)



## CHAPTER 23

# Maintenance Mode

- [Mobility Maintenance Mode Overview on page 592](#)
- [Changing a GTP Interface on page 593](#)
- [Deleting a GTP Interface on page 595](#)
- [Modifying an Access Point Name on page 596](#)
- [Configuring the Mobile Interface of an Access Point Name on page 598](#)
- [Deleting an Access Point Name on page 599](#)
- [Changing a Charging Profile on page 601](#)
- [Changing a Transport Profile on page 603](#)
- [Deleting a Charging Profile on page 605](#)
- [Deleting a Transport Profile on page 606](#)
- [Changing Address Attributes in the Mobile Address Pool on page 607](#)
- [Deleting a Mobile Address Pool on page 609](#)
- [Deleting a Session PIC on page 610](#)
- [Deleting a Services PIC on page 612](#)
- [Changing AMS Interface Parameters on page 614](#)
- [Changing Gateway Parameters with Maintenance Mode on page 617](#)
- [Example: Changing Access Point Name Values on page 619](#)
- [Example: Deleting an APN on page 620](#)
- [Example: Changing a Charging Profile on page 622](#)
- [Example: Changing a Transport Profile on page 624](#)
- [Example: Changing Mobility Pool Attributes on page 625](#)
- [Example: Deleting a Mobility Address Pool on page 631](#)
- [Example: Modifying Mobile Interface Parameters on page 633](#)
- [Example: Deleting a Session PIC on page 636](#)
- [Example: Deleting a Services PIC on page 640](#)
- [Example: Changing an AMS Interface on page 643](#)

## Mobility Maintenance Mode Overview

---

Junos OS maintenance mode for the MobileNext Broadband Gateway allows you to take certain network functionality offline to perform specific maintenance tasks without disrupting service. When access point names, gateways, subscribers, and the like need maintenance, entering maintenance mode prevents these mobility elements from accepting new requests. You have the option of allowing all existing services to complete, or clear them. When ready, proceed with critical maintenance functions with a minimum of service disruption. Subscribers who attempt to access a gateway that is active in maintenance mode are prompted with a notice that the service is not supported.

You must make the following changes in maintenance mode:

- Delete or modify the addresses of certain GPRS tunneling protocol (GTP) interfaces.
- Delete or change the type of an access point name (APN).
- Change mobile interface configuration parameters.
- Change a mobile interface for an APN.
- Delete or modify a charging profile.
- Delete or modify a policy and charging enforcement function (PCEF) profile.
- Delete or modify a transport profile.
- Delete a mobile pool or modify its parameters.

These maintenance tasks are discussed in this topic. You can perform all other maintenance tasks outside of maintenance mode.

Notice that the maintenance mode procedures listed do not include adding elements. New gateways, APNs, and such carry no traffic and thus do not need to be gracefully halted. However, you can create new mobility network elements in maintenance mode as an environment in which to test configurations before deploying them.

### Related Documentation

- [Changing a GTP Interface on page 593](#)
- [Deleting a GTP Interface on page 595](#)
- [Modifying an Access Point Name on page 596](#)
- [Configuring the Mobile Interface of an Access Point Name on page 598](#)
- [Deleting an Access Point Name on page 599](#)
- [Changing a Charging Profile on page 601](#)
- [Deleting a Charging Profile on page 605](#)
- [Changing a Transport Profile on page 603](#)
- [Deleting a Transport Profile on page 606](#)
- [Deleting a Session PIC on page 610](#)
- [Deleting a Services PIC on page 612](#)

- [Changing AMS Interface Parameters on page 614](#)
- [Changing Gateway Parameters with Maintenance Mode on page 617](#)

## Changing a GTP Interface

This procedure describes how to use maintenance mode to halt new sessions from being started and to verify that there are no active sessions remaining before making changes to a GPRS tunneling protocol (GTP) interface address.

1. Enter configuration mode in the CLI.

```
user@host> configure
```

2. Activate maintenance mode for a gateway.

```
user@host# set unified-edge gateways ggsn-pgw gw-name service-mode
maintenance"
```

3. Verify that the mobility gateway is in maintenance mode.

```
user@host# run show unified-edge ggsn-pgw gateway service-mode
```



**NOTE:** From the gateway hierarchy, the service mode for the gateway shows Maintenance – Active Phase if all the sessions using this pool are cleared. The service mode for the gateway shows Maintenance – In Phase if there are some sessions actively using this pool.

4. Verify that there are no subscribers active on this gateway.

```
user@host# run show unified-edge ggsn-pgw subscribers gateway gw-name
```



**NOTE:** If a large number of subscribers will use this gateway, the preceding command will be process intensive, in which case, you can use the following command:

```
user@host# run show unified-edge ggsn-pgw status
```

This command shows the active contexts across all of the gateway instances.

5. Verify that there are no outstanding CDRs for the gateway.

```
user@host# show unified-edge ggsn-pgw charging transfer status
```

6. (Optional) Terminate sessions that are using the gateway and clear CDRs using the following **clear** commands:

```
user@host# run clear unified-edge ggsn-pgw subscribers gateway gw-name
```

```
user@host# run clear unified-edge ggsn-pgw subscribers charging gateway gw-name
```



**CAUTION:** These clear commands clear all of the existing subscribers on the gateway. Only issue these commands if you intend to disconnect service to all these subscribers.

7. When the subscriber count is zero, all sessions have ended, and the charging data records (CDRs) are flushed, modify the GTP interface in active maintenance mode.

```
user@host# set unified-edge gateways ggsn-pgw gw-name gtp interface  
interface-name  
user@host# commit
```



**NOTE:** These modifications must be made in active maintenance mode or they will fail.

8. Verify that changes were properly committed.

```
user@host# run show configuration unified-edge ggsn-pgw gateway gw-name
```

9. Exit maintenance mode and commit.

```
user@host# delete unified-edge gateways ggsn-pgw gw-name gateway gw-name  
service-mode  
user@host# commit
```

10. Return the gateway to operational state.

```
user@host# run show unified-edge ggsn-pgw gateway service-mode
```

**Related  
Documentation**

- [Mobility Maintenance Mode Overview on page 592](#)
- [Deleting a GTP Interface on page 595](#)
- [Changing Gateway Parameters with Maintenance Mode on page 617](#)



## Deleting a GTP Interface

This procedure describes how to use maintenance mode to delete a GPRS tunneling protocol (GTP) interface. You must first halt new sessions from being started and verify that there are no active sessions remaining.

You can use maintenance mode to remove any of the following GTP interfaces:

- Gn
- Gp
- S5
- S8

You can also enter maintenance mode to delete control and data portions of these interface configurations.

1. Enter configuration mode in the CLI.

```
user@host> configure
```

2. Activate maintenance mode for a gateway.

3. Verify that the mobility gateway is in maintenance mode.

```
user@host# run show unified-edge ggsn-pgw gateway service-mode
```



**NOTE:** From the gateway hierarchy, the service mode for the gateway shows Maintenance – Active Phase if all the sessions using this pool are cleared. The service mode for the gateway shows Maintenance – In Phase if there are some sessions actively using this pool. The service mode for the gateway shows Maintenance – Out Phase if maintenance mode is not configured (that is, the gateway is in operational mode).

Verify that there are no subscribers active on this gateway.

```
user@host# run show unified-edge ggsn-pgw subscriber gateway gw-name
```

4. Verify that there are no outstanding CDRs for the gateway.

```
user@host# show unified-edge ggsn-pgw charging transfer status
```

5. (Optional) Terminate sessions that are using the gateway and clear CDRs using the following **clear** commands:

```
user@host# run clear unified-edge ggsn-pgw subscribers gateway gw-name
```

```
user@host# run clear unified-edge ggsn-pgw subscribers charging gateway gw-name
```

6. When the subscriber count is zero, all sessions have ended, and the charging data records (CDRs) are flushed, delete the GTP interface in active maintenance mode.



**NOTE:** These modifications must be made in active maintenance mode or they will fail.

7. Delete the GTP interface.

```
user@host# delete unified-edge gateways ggsn-pgw gw-name gtp interface  
interface-name  
user@host# commit
```

8. Exit maintenance mode and commit.

```
user@host# delete unified-edge gateways ggsn-pgw gw-name gateway gw-name  
service-mode  
user@host# commit
```

9. Verify that changes were properly committed.

```
user@host# run show configuration unified-edge ggsn-pgw gateway gw-name
```

#### Related Documentation

- [Mobility Maintenance Mode Overview on page 592](#)
- [Changing a GTP Interface on page 593](#)
- [Changing Gateway Parameters with Maintenance Mode on page 617](#)

---

## Modifying an Access Point Name

This procedure describes how to use maintenance mode to modify an access point name (APN). Options include modifying such parameters as *apn-type*, *mobile-interface*, *charging*, and *maximum-bearers*. You must first halt new sessions from being started and verify that there are no active sessions remaining.

To change an access point name:

1. Enter configuration mode in the CLI.

```
user@host> configure
```

2. Activate maintenance mode for an APN.

```
user@host# set unified-edge gateways ggsn-pgw gw-name apn-services apns  
apn-name service-mode maintenance
```

3. Commit the command.

```
user@host# commit
```

4. Verify that the APN is in maintenance mode.

```
user@host# run show unified-edge ggsn-pgw apn service-mode
```

This command displays the service-mode status for all the APNs. You can verify the status for the specific APN and take action accordingly.



**NOTE:** The service mode for the APN shows Maintenance – Active Phase if all the sessions using this APN are cleared. The service mode for the APN shows Maintenance - In Phase if there are some sessions actively using this APN.

5. Verify that there are no subscribers active on the APN.

```
user@host# run show unified-edge ggsn-pgw subscribers | match apn-name
```

6. (Optional) Terminate sessions on an APN using the **clear** command

```
user@host# run clear unified-edge ggsn-pgw subscribers apn apn-name gateway gw-name
```

7. When the subscriber count is zero and all sessions have ended, make and commit changes to the APN in active maintenance mode.



**NOTE:** These modifications must be made in active maintenance mode or they will fail.

8. Modify the APN and commit the changes.

9. Exit maintenance mode.

```
user@host# delete unified-edge gateways ggsn-pgw gw-name apn-services apns apn-name service--mode
user@host# commit
```

10. Verify that changes were properly committed.

```
user@host# run show configuration unified-edge gateways ggsn-pgw gw-name apn-services apns apn-name
```

The APN edits should appear in the show command output.

11. Return the gateway to operational state.

```
user@host# run show unified-edge ggsn-pgw gateway service-mode
```



**NOTE:** Although maintenance mode does not explicitly include AAA options, certain AAA changes require you to place affected APNs in maintenance mode first. These changes include: changing an AAA profile name and changing authorization or accounting elements. If you attempt to make AAA changes that affect an APN that is not in maintenance mode, you are prompted to place the appropriate APN into maintenance mode before proceeding with AAA profile name or element changes.

#### Related Documentation

- [Mobility Maintenance Mode Overview on page 592](#)
- [Configuring the Mobile Interface of an Access Point Name on page 598](#)
- [Deleting an Access Point Name on page 599](#)

- [Changing Gateway Parameters with Maintenance Mode on page 617](#)

## Configuring the Mobile Interface of an Access Point Name

---

This procedure describes how to use maintenance mode to modify attributes of the mobile interface for an access point name (APN). You must first halt new sessions from being started and verify that there are no active sessions remaining.

To configure the mobile interface of an access point name:

1. Enter configuration mode in the CLI.

```
user@host> configure
```

2. Activate maintenance mode for the APN using the mobile interface to be modified.

```
user@host# set unified-edge gateways ggsn-pgw gw-name apn-services apns  
apn-name service-mode maintenance  
user@host# commit
```

3. Verify that the APN of this mobile interface is in maintenance mode.

```
user@host# run show unified-edge ggsn-pgw apn service-mode
```



**NOTE:** From the gateway hierarchy, the service mode for the gateway shows Maintenance – Active Phase if all the sessions using this APN are cleared. The service mode for the gateway shows Maintenance – In Phase if there are some sessions actively using this APN. The service mode for the APN shows Maintenance – Out Phase if maintenance mode is not configured (that is, it is in operational mode).



**NOTE:** You cannot make and commit changes to a mobile interface unless the APN to which it is attached is in maintenance mode.

4. Verify that there are no subscribers active on the APN.

```
user@host# run show unified-edge ggsn-pgw subscribers | match apn-name
```

5. (Optional) Terminate sessions that are using a mobile pool using the **clear** command.

```
user@host# run clear unified-edge ggsn-pgw subscribers apn apn-name gateway  
gw-name
```

6. When the subscriber count is zero and all sessions have ended, make and commit changes to the APN mobile interface in active maintenance mode.



**NOTE:** These modifications must be made in active maintenance mode or they will fail.

7. Modify the interface and commit the changes.

- Exit maintenance mode.

```
user@host# delete unified-edge gateways ggsn-pgw gw-name apn-services apns
apn-name service-mode
user@host# commit
```

- Verify that changes were properly committed.

```
user@host# run show configuration unified-edge gateways ggsn-pgw gw-name
apn-services apns apn-name
```

- Return the gateway to operational state.

```
user@host# run show unified-edge ggsn-pgw gateway service-mode
```

#### Related Documentation

- [Mobility Maintenance Mode Overview on page 592](#)
- [Example: Changing Access Point Name Values on page 619](#)
- [Deleting an Access Point Name on page 599](#)
- [Changing Gateway Parameters with Maintenance Mode on page 617](#)

## Deleting an Access Point Name

This procedure describes how to use maintenance mode to delete an access point name (APN). You must first halt new sessions from being started and verify that there are no active sessions remaining.

To delete an access point name:

- Enter configuration mode in the CLI.

```
user@host> configure
```

- Activate maintenance mode for an APN.

```
user@host# set unified-edge gateways ggsn-pgw gw-name apn-services apn apn-name
service-mode maintenance
user@host# commit
```

- Verify that the APN is in maintenance mode.

```
user@host# run show unified-edge ggsn-pgw apn service-mode
```



**NOTE:** The service mode for the APN shows Maintenance – Active Phase if all the sessions using this APN are cleared. The service mode for the APN shows Maintenance – In Phase if there are some sessions actively using this APN. The service mode for the APN shows Maintenance – Out Phase if maintenance mode is not configured (that is, it is in operational mode).

- Verify that there are no subscribers active on the APN.

```
user@host# run show unified-edge ggsn-pgw apn apn-name gateway gw-name
```

- (Optional) Terminate sessions that are using an APN using the **clear** command.

```
user@host# run clear unified-edge ggsn-pgw subscribers apn apn-name gateway  
gw-name
```

6. When the subscriber count is zero and all sessions have ended, delete the APN in active maintenance mode.



**NOTE:** These modifications must be made in active maintenance mode or they will fail.

7. Delete the APN and commit the changes.

```
user@host# delete unified-edge gateways ggsn-pgw gw-name apn-services apns  
apn-name
```

8. Verify that changes were properly committed by showing the configuration for the entire unified edge to make sure the APN is deleted.
9. Return the gateway to the operational state.

```
user@host# run show unified-edge ggsn-pgw gateway service-mode
```

**Related  
Documentation**

- [Mobility Maintenance Mode Overview on page 592](#)
- [Configuring the Mobile Interface of an Access Point Name on page 598](#)
- [Example: Changing Access Point Name Values on page 619](#)
- [Changing Gateway Parameters with Maintenance Mode on page 617](#)

## Changing a Charging Profile

This procedure describes how to use maintenance mode to change a charging profile. You must first prevent new sessions from being started and verify that there are no active sessions remaining.

You can modify the following attributes of a charging profile only when the charging profile is in maintenance mode:

- CDR profile
- Charging profile identifier (ID)
- Transport profile
- Trigger profile

To change the charging profile:



**NOTE:** The following configuration steps are applicable at both the [edit unified-edge gateways ggsn-pgw *gateway-name* charging] and the [edit unified-edge gateways sgw *gateway-name* charging] hierarchy levels. However, for clarity, they are presented only at the [edit unified-edge gateways ggsn-pgw *gateway-name* charging] hierarchy level. Unless explicitly stated otherwise, the configuration steps can be used with exactly the same syntax at both hierarchy levels.

For clear and show commands, obtain the S-GW command by replacing ggsn-pgw with sgw in the clear or show command.

1. Enter configuration mode in the CLI.

```
user@host> configure
```

2. Activate maintenance mode for the charging profile.

```
user@host# set unified-edge gateways ggsn-pgw gw-name charging charging-profiles
  profile-name service-mode maintenance
user@host# commit
```

3. Verify that the charging profile is in maintenance mode.

```
user@host# run show unified-edge ggsn-pgw charging service-mode gateway
  gateway-name charging-profile profile-name
```



**NOTE:** The service mode for the charging profile shows Maintenance – Active Phase if all the sessions using this profile are cleared. The service mode for the charging profile shows Maintenance – In Phase if some sessions are actively using this profile. The service mode for the profile shows Maintenance – Out Phase if maintenance mode is not configured (that is, it is in operational mode).

4. Verify that there are no active subscribers for the charging profile.

```
user@host# run show unified-edge ggsn-pgw subscribers charging gateway gw-name
charging-profile profile-name
```

5. (Optional) Use the **clear** command to terminate subscribers using the charging profile.

```
user@host# run clear unified-edge ggsn-pgw subscribers charging gateway gw-name
charging-profile profile-name
```

When the subscriber count is zero and all sessions have ended, you can make and commit changes to the charging profile in active maintenance mode.

6. Modify the charging profile as required.



**NOTE:** These modifications must be made in active maintenance mode or they will fail.

7. Commit the changes and verify that they are properly committed.

```
user@host# commit
user@host# show unified-edge ggsn-pgw gw-name charging charging-profile
profile-name
```

8. Exit maintenance mode and commit to return to normal operations.

```
user@host# delete unified-edge gateways ggsn-pgw gw-name charging
charging-profile profile-name service-mode
user@host# commit
```

#### Related Documentation

- [Changing a Transport Profile on page 603](#)
- [Changing Gateway Parameters with Maintenance Mode on page 617](#)
- [Deleting a Charging Profile on page 605](#)
- [Example: Changing a Charging Profile on page 622](#)
- [Mobility Maintenance Mode Overview on page 592](#)



## Changing a Transport Profile

This procedure describes how to use maintenance mode to change a transport profile. You must first prevent new sessions from being started and verify that there are no active sessions remaining.

You can modify the following attribute of a transport profile only when the transport profile is in maintenance mode:

- **cdr-release**

To change a transport profile:



**NOTE:** The following configuration steps are applicable at both the [edit unified-edge gateways ggsn-pgw *gateway-name* charging] and the [edit unified-edge gateways sgw *gateway-name* charging] hierarchy levels. However, for clarity, they are presented only at the [edit unified-edge gateways ggsn-pgw *gateway-name* charging] hierarchy level. Unless explicitly stated otherwise, the configuration steps can be used with exactly the same syntax at both hierarchy levels.

For clear and show commands, obtain the S-GW command by replacing ggsn-pgw with sgw in the clear or show command.

1. Enter configuration mode in the CLI.

```
user@host> configure
```

2. Activate maintenance mode for the transport profile.

```
user@host# set unified-edge gateways ggsn-pgw gw-name charging transport-profiles
  profile-name service-mode maintenance
user@host# commit
```

3. Verify that the transport profile is in maintenance mode.

```
user@host# run show unified-edge ggsn-pgw charging service-mode gateway gw-name
transport-profile profile-name
```



**NOTE:** The service mode for the transport profile shows Maintenance – Active Phase if all the sessions using this profile are cleared. The service mode for a transport profile shows Maintenance – In Phase if some sessions are actively using this profile. The service mode for the profile shows Maintenance – Out Phase if maintenance mode is not configured (that is, it is in operational mode).

4. Verify that there are no active subscribers on this transport profile.

```
user@host# run show unified-edge ggsn-pgw subscribers charging gateway gw-name
transport-profile profile-name
```

5. (Optional) Use the **clear** command to terminate subscribers using the transport profile.

```
user@host# run clear unified-edge ggsn-pgw subscribers charging transport-profile  
profile-name gateway gw-name
```

When the subscriber count is zero and all sessions have ended, you can make and commit changes to the transport profile in active maintenance mode.

6. Modify the transport profile as required.



**NOTE:** These modifications must be made in active maintenance mode or they will fail.

7. Commit the changes and verify that they are properly committed.

```
user@host# commit  
user@host# show unified-edge ggsn-pgw gw-name charging transport-profile  
profile-name
```

8. Exit maintenance mode and commit.

```
user@host# delete unified-edge gateways ggsn-pgw gw-name charging  
transport-profile profile-name service-mode  
user@host# commit
```

#### Related Documentation

- [Changing a Charging Profile on page 601](#)
- [Changing Gateway Parameters with Maintenance Mode on page 617](#)
- [Deleting a Transport Profile on page 606](#)
- [Example: Changing a Transport Profile on page 624](#)
- [Mobility Maintenance Mode Overview on page 592](#)

## Deleting a Charging Profile

This procedure describes how to use maintenance mode to delete a charging profile. You must first prevent new sessions from being started and verify that there are no active sessions remaining.

To delete a charging profile:



**NOTE:** The following configuration steps are applicable at both the [edit unified-edge gateways ggsn-pgw *gateway-name* charging] and the [edit unified-edge gateways sgw *gateway-name* charging] hierarchy levels. However, for clarity, they are presented only at the [edit unified-edge gateways ggsn-pgw *gateway-name* charging] hierarchy level. Unless explicitly stated otherwise, the configuration steps can be used with exactly the same syntax at both hierarchy levels.

For clear and show commands, obtain the S-GW command by replacing ggsn-pgw with sgw in the clear or show command.

1. Enter configuration mode in the CLI.

```
user@host> configure
```

2. Activate maintenance mode for a charging profile.

```
user@host# set unified-edge gateways ggsn-pgw gw-name charging charging-profiles
  profile-name service-mode maintenance
commit
```

3. Verify that the charging profile is in maintenance mode.

```
user@host#run show unified-edge ggsn-pgw charging service-mode gateway gw-name
charging-profile profile-name
```



**NOTE:** The service mode for the charging profile shows Maintenance – Active Phase if all the sessions using this pool are cleared. The service mode for the charging profile shows Maintenance – In Phase if some sessions are actively using this profile. The service mode for the charging profile shows Maintenance – Out Phase if maintenance mode is not configured (that is, it is in operational mode).

4. Verify that there are no active subscribers for the charging profile.

```
user@host#run show unified-edge ggsn-pgw subscribers charging gateway gw-name
charging-profile profile-name
```

5. (Optional) Use the clear command to terminate subscribers using the charging profile.

```
user@host# run clear unified-edge ggsn-pgw subscribers charging charging-profile
  profile-name gateway gw-name
```

When the subscriber count is zero and all sessions have ended, you can make and commit changes to the charging profile in active maintenance mode.

6. Delete the charging profile and commit the changes.

```
user@host# delete unified-edge gateways ggsn-pgw gw-name charging
charging-profile profile-name
user@host# commit
```

7. Verify that the changes are properly committed.

```
user@host# show unified-edge ggsn-pgw gw-name charging
```

#### Related Documentation

- [Changing a Charging Profile on page 601](#)
- [Changing Gateway Parameters with Maintenance Mode on page 617](#)
- [Changing a Transport Profile on page 603](#)
- [Example: Changing a Charging Profile on page 622](#)
- [Mobility Maintenance Mode Overview on page 592](#)

---

## Deleting a Transport Profile

This procedure describes how to use maintenance mode to delete a transport profile. You must first prevent new sessions from being started and verify that there are no active sessions remaining.

To delete a transport profile:



**NOTE:** The following configuration steps are applicable at both the [edit unified-edge gateways ggsn-pgw *gateway-name* charging] and the [edit unified-edge gateways sgw *gateway-name* charging] hierarchy levels. However, for clarity, they are presented only at the [edit unified-edge gateways ggsn-pgw *gateway-name* charging] hierarchy level. Unless explicitly stated otherwise, the configuration steps can be used with exactly the same syntax at both hierarchy levels.

For clear and show commands, obtain the S-GW command by replacing ggsn-pgw with sgw in the clear or show command.

1. Enter configuration mode in the CLI.

```
user@host> configure
```

2. Activate maintenance mode for the transport profile.

```
user@host# set unified-edge gateways ggsn-pgw gw-name charging transport-profiles
profile-name service-mode maintenance
commit
```

3. Verify that the transport profile is in maintenance mode.

```
user@host# run show unified-edge ggsn-pgw charging service-mode gateway gw-name
transport-profile profile-name
```



**NOTE:** The service mode for the transport profile shows Maintenance – Active Phase if all the sessions using this pool are cleared. The service mode for the transport profile shows Maintenance – In Phase if some sessions are actively using this profile. The service mode for the transport profile shows Maintenance – Out Phase if maintenance mode is not configured (that is, it is in operational mode).

4. Verify that there are no active subscribers on the transport profile.

```
user@host# run show unified-edge ggsn-pgw subscribers charging gateway gw-name
transport-profile profile-name
```

5. (Optional) Use the **clear** command to terminate subscribers using the transport profile.

```
user@host# run clear unified-edge ggsn-pgw subscribers charging transport-profile
profile-name gateway gw-name
```

When the subscriber count is zero and all sessions have ended, you can make and commit changes to the transport profile in active maintenance mode.

6. Delete the transport profile and commit the changes.

```
user@host# delete unified-edge gateways ggsn-pgw gw-name charging
transport-profile profile-name
user@host# commit
```

7. Verify that the changes are properly committed.

```
user@host# show unified-edge ggsn-pgw gw-name charging
```

#### Related Documentation

- [Changing a Charging Profile on page 601](#)
- [Changing Gateway Parameters with Maintenance Mode on page 617](#)
- [Changing a Transport Profile on page 603](#)
- [Example: Changing a Transport Profile on page 624](#)
- [Mobility Maintenance Mode Overview on page 592](#)

## Changing Address Attributes in the Mobile Address Pool

This procedure describes how to place a mobile pool of a virtual routing and forwarding (VRF) instance in maintenance mode, allow all existing sessions using this pool to gracefully terminate, and then delete or modify pool attributes (for example, change address ranges in a pool).

To change address attributes in the mobile address pool:

1. Enter configuration mode in the CLI.

```
user@host> configure
```

2. Activate maintenance mode for a mobile pool.

```
user@host# configure
user@host# set routing-instance vrf-name access address-assignment mobile pools
juniper-pool service-mode maintenance
user@host# commit
```

3. Verify that all subscriber sessions have ended.

```
user@host# run show unified-edge ggsn-pgw address-assignment pool brief
```



**NOTE:** The service mode shows Maintenance – Active Phase if all the sessions are cleared. The service mode shows Maintenance – In Phase if there are some sessions active. The service mode shows Maintenance – Out Phase if maintenance mode is not configured (that is, it is in operational mode).

4. (Optional) Terminate existing sessions using the **clear** command.

```
user@host# configure
user@host# run clear unified-edge ggsn-pgw subscribers routing-instance juniper-vrf
```



**NOTE:** When the subscriber count is zero and all sessions have terminated, the service mode status indicates Maintenance – Active phase. In this state, you can modify mobile pool attributes and commit changes.

5. Make changes to the pool and commit.
6. Verify that changes were properly committed.

```
user@host# run show configuration routing-instance access address-assignment
mobile-pools pool-name detail
```



**NOTE:** These modifications, if made outside of active maintenance mode, will fail.

7. Exit maintenance mode to return to normal operational mode.

```
user@host# delete routing-instance juniper-vrf access address-assignment
mobile-pools pool-name service-mode
user@host# commit
```

8. Return the gateway to operational state.

```
user@host# run show unified-edge ggsn-pgw gateway service-mode
```

#### Related Documentation

- [Mobility Maintenance Mode Overview on page 592](#)
- [Deleting a Mobile Address Pool on page 609](#)

## Deleting a Mobile Address Pool

This procedure describes how to delete a mobile pool. You must first halt new sessions from being started and verify that there are no active sessions remaining. The steps are similar to those described in [“Changing Address Attributes in the Mobile Address Pool” on page 607](#)

To delete an address from an address pool:

1. Enter configuration mode in the CLI.

```
user@host> configure
```

2. Activate maintenance mode for a mobile pool.

```
user@host# set routing-instance juniper-vrf access address-assignment mobile-pools
pool-name service-mode maintenance
commit
```

3. Verify that all subscriber sessions have ended.

```
user@host# run show unified-edge ggsn-pgw address-assignment pool brief
```



**NOTE:** The service mode shows Maintenance – Active Phase if all the sessions are cleared. The service mode shows Maintenance – In Phase if there are some sessions active. The service mode shows Maintenance – Out Phase if maintenance mode is not configured (that is, it is in operational mode).

4. (Optional) Terminate sessions that are using a mobile pool using the **clear** command.

```
user@host# configure
user@host# run clear unified-edge ggsn-pgw subscribers routing-instance juniper-vrf
```



**NOTE:** When the subscriber count is zero and all sessions have terminated, the service mode status will indicate “Maintenance – Active phase.” In this state, you can modify pool attributes and commit changes.

5. For this pool, when the subscriber count is zero and all sessions have ended, the service mode status indicates “Maintenance – Active Phase.” In this state, you can modify mobile pool attributes and commit changes.



**NOTE:** These modifications, if made outside of active maintenance mode, will fail.

6. Delete the address pool and commit the change.

```
user@host# delete routing-instance juniper-vrf access address-assignment
mobile-pools juniper-pool
commit
```

7. Verify that the address pool has been deleted (that is, it is not listed in the output).

```
user@host# run show configuration routing-instance juniper-vrf access
address-assignment mobile-pools juniper-pool
user@host# commit
```

- Related Documentation**
- [Mobility Maintenance Mode Overview on page 592](#)
  - [Changing Address Attributes in the Mobile Address Pool on page 607](#)

---

## Deleting a Session PIC

This procedure shows how to delete a session PIC using maintenance mode at the **[edit unified-edge gateways ggsn-pgw *ggsn-pgw-name* system session-pics interface]** or **[edit unified-edge gateways sgw *sgw-name* system session-pics interface]** hierarchy level. The session PIC can be an aggregated multiservices interface (AMS). Session PICs process control plane messages on a broadband gateway.

Before you delete a session PIC using maintenance mode:

- Make sure that this change has been coordinated with affected groups and users.

To configure maintenance mode and session PIC deletion:

1. Verify the current status of maintenance mode for this session PIC.

```
user@host> show unified-edge ggsn-pgw gateway-name system interfaces
service-mode
user@host> show unified-edge sgw gateway-name system interfaces service-mode
```



**NOTE:** The **service-mode** option displays the information details about maintenance mode as well as status.

---

### Maintenance Mode

MM Active Phase - System is ready to accept configuration changes for all attributes of this object and its sub-hierarchies.

MM In/Out Phase - System is ready to accept configuration changes only for non-maintenance mode attributes of this object and its sub-hierarchies.

### Interface Name Gateway Name Service Mode

ms-1/0/0	MBG1	Operational
ms-1/1/0	MBG1	Operational
ms-2/0/0	MBG1	Operational
ms-2/1/0	MBG1	Operational
pfe-0/0/0	MBG1	Operational
pfe-0/1/0	MBG1	Operational
pfe-0/2/0	MBG1	Operational
pfe-0/3/0	MBG1	Operational
ams1	MBG1	Operational

2. Place the broadband gateway in configuration mode.



```
user@host# configure
```

3. On the Gateway GPRS Support Node (GGSN). Packet Data Network Gateway (P-GW), or Serving Gateway (S-GW), place the interface in maintenance mode.

```
user@host# set unified-edge gateways ggsn-pgw gateway-name system session-pics
interface interface-name service-mode maintenance
```

```
user@host# set unified-edge gateways sgw gateway-name system session-pics
interface interface-name service-mode maintenance
```

4. Commit maintenance mode.

```
user@host# commit
```

5. Verify that the session PIC is in active maintenance mode where configuration changes will be accepted for this object and all of its subhierarchies.

```
user@MBG1> show unified-edge ggsn-pgw gateway-name system interfaces
service-mode
```

```
user@MBG1> show unified-edge sgw gateway-name system interfaces service-mode
```

#### Maintenance Mode

MM Active Phase - System is ready to accept configuration changes for all attributes of this object and its sub-hierarchies.

MM In/Out Phase - System is ready to accept configuration changes only for non-maintenance mode attributes of this object and its sub-hierarchies.

Interface Name	Gateway Name	Service Mode
ms-1/0/0	MBG1	Operational
ms-1/1/0	MBG1	Maintenance - Active Phase
ms-2/0/0	MBG1	Operational
ms-2/1/0	MBG1	Operational
pfe-0/0/0	MBG1	Operational
pfe-0/1/0	MBG1	Operational
pfe-0/2/0	MBG1	Operational
pfe-0/3/0	MBG1	Operational
ams1	MBG1	Operational



**NOTE:** All subscribers serviced by the session PIC must go to zero. All Charging Data Records (CDRs) for these subscribers must be flushed out. You can wait for these conditions to be met, or use the clear command for the interface (or gateway) to force these conditions.

6. Delete the session PIC.

```
user@host# delete unified-edge gateways ggsn-pgw gateway-name system interface
interface-name
```

```
user@host# delete unified-edge gateways sgw gateway-name system interface
interface-name
```

7. Exit with commit.



**NOTE:** Deletion of a session PIC automatically exits maintenance mode for the deleted PIC.

user@host# commit

#### Related Documentation

- [Mobility Maintenance Mode Overview on page 592](#)
- [Deleting a Services PIC on page 612](#)
- [Changing AMS Interface Parameters on page 614](#)
- [Changing Gateway Parameters with Maintenance Mode on page 617](#)

---

## Deleting a Services PIC

This procedure shows how to delete a services PIC using maintenance mode at the **[edit unified-edge gateways ggsn-pgw ggsn-pgw-name system session-pics interface]** or **[edit unified-edge gateways sgw sgw-name system session-pics interface]** hierarchy level. The services PIC can be an aggregated multiservices interface (AMS). Services PICs perform packet-related services on a broadband gateway.

Before you delete a services PIC using maintenance mode:

- Make sure that this change has been coordinated with affected groups and users.

To configure maintenance mode and services PIC deletion:

1. Verify the current status of maintenance mode for this services PIC.

```
user@host> show unified-edge ggsn-pgw gateway-name system interfaces  
service-mode
```

```
user@host> show unified-edge sgw gateway-name system interfaces service-mode
```



**NOTE:** The service-mode option displays the information details about maintenance mode as well as status.

#### Maintenance Mode

MM Active Phase - System is ready to accept configuration changes for all attributes of this object and its sub-hierarchies.

MM In/Out Phase - System is ready to accept configuration changes only for non-maintenance mode attributes of this object and its sub-hierarchies.

Interface Name	Gateway Name	Service Mode
ms-1/0/0	MBG1	Operational
ms-1/1/0	MBG1	Operational
ms-2/0/0	MBG1	Operational
ms-2/1/0	MBG1	Operational
pfe-0/0/0	MBG1	Operational
pfe-0/1/0	MBG1	Operational

```
pfe-0/2/0 MBG1 Operational
pfe-0/3/0 MBG1 Operational
ams1 MBG1 Operational
```

2. Place the broadband gateway in configuration mode.

```
user@host# configure
```

3. On the Gateway GPRS Support Node (GGSN), Packet Data Network Gateway (P-GW), or Serving Gateway (S-GW), place the interface in maintenance mode.

```
user@host# set unified-edge gateways ggsn-pgw gateway-name system session-pics
interface interface-name service-mode maintenance
user@host# set unified-edge gateways sgw gateway-name system session-pics
interface interface-name service-mode maintenance
```

4. Commit maintenance mode.

```
user@host# commit
```

5. Verify that the services PIC is in active maintenance mode where configuration changes will be accepted for this object and all of its subhierarchies.

```
user@MGB1> show unified-edge ggsn-pgw gateway-name system interfaces
service-mode
user@MGB1> show unified-edge sgw gateway-name system interfaces service-mode
```

#### Maintenance Mode

MM Active Phase - System is ready to accept configuration changes for all attributes of this object and its sub-hierarchies.

MM In/Out Phase - System is ready to accept configuration changes only for non-maintenance mode attributes of this object and its sub-hierarchies.

```
Interface Name Gateway Name Service Mode
ms-1/0/0 MBG1 Operational
ms-1/1/0 MBG1 Operational
ms-2/0/0 MBG1 Maintenance - Active Phase
ms-2/1/0 MBG1 Operational
pfe-0/0/0 MBG1 Operational
pfe-0/1/0 MBG1 Operational
pfe-0/2/0 MBG1 Operational
pfe-0/3/0 MBG1 Operational
ams1 MBG1 Operational
```



**NOTE:** All subscribers serviced by the services PIC must go to zero. All Charging Data Records (CDRs) for these subscribers must be flushed out. You can wait for these conditions to be met, or use the clear command for the interface (or gateway) to force these conditions.

6. Delete the services PIC.

```
user@host# delete unified-edge gateways ggsn-pgw gateway-name system interface
interface-name
user@host# delete unified-edge gateways sgw gateway-name system interface
interface-name
```

7. Exit maintenance mode and commit.



**NOTE:** Deletion of a services PIC automatically exits maintenance mode for the deleted PIC.

```
user@host# commit
```

**Related  
Documentation**

- [Mobility Maintenance Mode Overview on page 592](#)
- [Deleting a Session PIC on page 610](#)
- [Changing AMS Interface Parameters on page 614](#)
- [Changing Gateway Parameters with Maintenance Mode on page 617](#)

---

## Changing AMS Interface Parameters

This procedure shows how to change the parameters for an aggregated multiservices (AMS) interface on a MobileNext Broadband Gateway using maintenance mode at the **[edit interfaces]** hierarchy level. If an AMS interface is configured under a gateway's session PICs or services PICs, and there is a change to any load-balancing options such as membership of AMS interfaces (**mams-**), then the AMS interface must be in maintenance mode.

Before you change AMS parameters using maintenance mode:

- Make sure that this change has been coordinated with affected groups and users.

To configure maintenance mode and AMS parameter change:

1. Verify the current status of maintenance mode for the AMS.

```
user@MGB1> show unified-edge ggsn-pgw gateway-name system interfaces  
service-mode
```



**NOTE:** The service-mode option displays the information details about maintenance mode as well as status.

### Maintenance Mode

MM Active Phase - System is ready to accept configuration changes for all attributes of this object and its sub-hierarchies.

MM In/Out Phase - System is ready to accept configuration changes only for non-maintenance mode attributes of this object and its sub-hierarchies.

Interface Name	Gateway Name	Service Mode
ms-1/0/0	MBG1	Operational
ms-1/1/0	MBG1	Operational
ms-2/0/0	MBG1	Operational
ms-2/1/0	MBG1	Operational

```

pfe-0/0/0 MBG1 Operational
pfe-0/1/0 MBG1 Operational
pfe-0/2/0 MBG1 Operational
pfe-0/3/0 MBG1 Operational
ams1 MBG1 Operational

```

- Place the broadband gateway in configuration mode.

```
user@host# configure
```

- Show the current configuration for the AMS interface

```

user@host# show interfaces interface-name
load-balancing-options {
  member-interface mams-4/1/0;
  member-interface mams-5/1/0;
  member-failure-options {
    redistribute-all-traffic {
      enable-rejoin;
    }
  }
  high-availability-options {
    many-to-one {
      preferred-backup mams-5/1/0;
    }
  }
}
unit 1 {
  family inet;
}
unit 2 {
  family inet;
}

```

- On the gateway, place the interface in maintenance mode.

```

user@host# set unified-edge ggsn-pgw gateway-name system interface interface-name
service-mode maintenance

```



**NOTE:** This is done at the [edit unified-edge] hierarchy level.

- Commit maintenance mode.

```
user@host# commit
```

- Verify that the AMS interface is in active maintenance mode where configuration changes will be accepted for this object and all of its subhierarchies.

```

user@MGB1> show unified-edge ggsn-pgw gateway-name system interfaces
service-mode

```

#### Maintenance Mode

MM Active Phase - System is ready to accept configuration changes for all attributes of this object and its sub-hierarchies.

MM In/Out Phase - System is ready to accept configuration changes only for non-maintenance mode attributes of this object and its sub-hierarchies.

Interface Name	Gateway Name	Service Mode
ms-1/0/0	MBG1	Operational
ms-1/1/0	MBG1	Operational
ms-2/0/0	MBG1	Operational
ms-2/1/0	MBG1	Operational
pfe-0/0/0	MBG1	Operational
pfe-0/1/0	MBG1	Operational
pfe-0/2/0	MBG1	Operational
pfe-0/3/0	MBG1	Operational
ams1	MBG1	Maintenance - Active Phase



**NOTE:** All subscribers serviced by the AMS interface must go to zero. All Charging Data Records (CDRs) for these subscribers must be flushed out. You can wait for these conditions to be met, or use the clear command for the interface (or gateway) to force these conditions.

7. Delete or change AMS member interfaces and parameters.

```
user@MGB1> show unified-edge ggsn-pgw gateway-name system interfaces
service-mode
user@host# delete unified-edge ggsn-pgw gateway-name system interface
interface-name load-balancing-options member-interface mams-interface-name
user@host# set interfaces interface-name load-balancing-options member-interface
mams-interface-name
user@host# delete interfaces interface-name load-balancing-options
high-availability-options many-to-one preferred-backup mams-interface-name
user@host# set interfaces interface-name load-balancing-options
high-availability-options many-to-one preferred-backup mams-interface-name
```



**NOTE:** This procedure requires operations at the [edit unified-edge] and [edit interfaces] hierarchy level. Be careful!

8. Exit maintenance mode and commit.

```
user@host# delete unified-edge ggsn-pgw gateway-name system interface
interface-name service-mode maintenance
user@host# commit
```

**Related  
Documentation**

- [Mobility Maintenance Mode Overview on page 592](#)
- [Deleting a Session PIC on page 610](#)
- [Deleting a Services PIC on page 612](#)
- [Changing Gateway Parameters with Maintenance Mode on page 617](#)

## Changing Gateway Parameters with Maintenance Mode

This procedure shows how to change the parameters for a General GPRS Support Node (GGSN), Packet Data Network Gateway (P-GW), or Service Gateway (S-GW) configured on a MobileNext Broadband Gateway using maintenance mode at the **[edit unified-edge gateways ggsn-pgw gateway-name]** (GGSN or P-GW) or **[edit unified-edge gateways sgw gateway-name]** (S-GW) hierarchy level.

The gateway must be in maintenance mode to change:

- Maximum number of bearers (GGSN, P-GW, or S-GW)
- Maximum number of network-behind-the-mobile (NBM) IPv4 prefixes for an anchor Packet Forwarding Engine (GGSN or P-GW)
- Maximum number of network-behind-the-mobile (NBM) IPv6 prefixes for an anchor Packet Forwarding Engine (GGSN or P-GW)
- Guaranteed bandwidth for each anchor Packet Forwarding Engine (S-GW)
- Maximum number of default bearers allowed (as a percentage of total bearers) on each anchor Packet Forwarding Engine (S-GW)
- Maximum number of bearers allowed on each anchor Packet Forwarding Engine (S-GW)

Before you change these gateway parameters using maintenance mode:

- Make sure that this change has been coordinated with affected groups and users.
- Make sure that this change will be applied to the correct gateway type and name.

To configure maintenance mode for a gateway parameter change:

1. Verify the current status of maintenance mode for the gateway. Under normal operating conditions, the service mode is **Operational** (that is, not in maintenance mode).

```
user@host> show unified-edge ggsn-pgw gateway-name service-mode
user@host> show unified-edge sgw gateway-name service-mode
```



**NOTE:** The **service-mode** option displays the information details about maintenance mode as well as status.

### Maintenance Mode

MM Active Phase - System is ready to accept configuration changes for all attributes of this object and its sub-hierarchies.

MM In/Out Phase - System is ready to accept configuration changes only for non-maintenance mode attributes of this object and its sub-hierarchies.

Gateway Name    Service Mode

<gateway-name> Operational

2. Place the broadband gateway in configuration mode.

```
user@host# configure
```

3. Place the gateway in maintenance mode.

```
user@host# set unified-edge ggsn-pgw gateway-name service-mode maintenance
user@host# set unified-edge sgw gateway-name service-mode maintenance
```

4. Commit maintenance mode.

```
user@host# commit
```

5. Verify that the gateway is in active maintenance mode where configuration changes will be accepted for this object.

```
user@host> show unified-edge ggsn-pgw gateway-name service-mode
user@host> show unified-edge sgw gateway-name service-mode
```



**NOTE:** The service-mode option displays the information details about maintenance mode as well as status.

#### Maintenance Mode

MM Active Phase - System is ready to accept configuration changes for all attributes of this object and its sub-hierarchies.

MM In/Out Phase - System is ready to accept configuration changes only for non-maintenance mode attributes of this object and its sub-hierarchies.

#### Gateway Name Service Mode

<gateway-name> Maintenance - Active Phase



**NOTE:** All subscribers serviced by the gateway must go to zero. All Charging Data Records (CDRs) for these subscribers must be flushed out. You can wait for these conditions to be met, or use the clear command for the gateway to force these conditions.

6. Set the new parameter values.

```
user@host# set unified-edge ggsn-pgw gateway-name maximum-bearers
maximum-bearers-value
user@host# set unified-edge sgw gateway-name maximum-bearers
maximum-bearers-value
```

```
user@host# set unified-edge ggsn-pgw gateway-name anchor-pfe-ipv4-nbm-prefixes
maximum-ipv4-prefixes
```

```
user@host# set unified-edge ggsn-pgw gateway-name anchor-pfe-ipv6-nbm-prefixes
maximum-ipv6-prefixes
```



```
user@host# set unified-edge sgw gateway-name anchor-pfe-guaranteed-bandwidth
anchor-pfe-guaranteed-bandwidth-value
```

```
user@host# set unified-edge sgw gateway-name
anchor-pfe-default-bandwidth-percentage
anchor-pfe-default-bandwidth-percentage-value
```

```
user@host# set unified-edge sgw gateway-name anchor-pfe-maximum-bearers
maximum-bearers-value
```

7. Exit maintenance mode and commit.

```
user@host# delete unified-edge ggsn-pgw gateway-name service-mode maintenance
user@host# delete unified-edge sgw gateway-name service-mode maintenance
user@host# commit
```

#### Related Documentation

- [Mobility Maintenance Mode Overview on page 592](#)
- [Deleting a Session PIC on page 610](#)
- [Deleting a Services PIC on page 612](#)
- [Changing AMS Interface Parameters on page 614](#)

## Example: Changing Access Point Name Values

- [Requirements on page 619](#)
- [Overview on page 619](#)
- [Configuration on page 619](#)

### Requirements

This example uses the following hardware and software components:

- An operational MX Series chassis
- Junos OS MobileNext Broadband Gateway package

### Overview

The following configuration example shows how to change an access point name (APN).

### Configuration

#### Step-by-Step Procedure

To change an APN configuration:

1. Verify the current status of maintenance mode for this APN profile.

```
user@host# run show unified-edge ggsn-pgw MBG1 apn-services apn Central
service-mode
```

```
Profile Name : Central
Service Mode : Operational
```

2. Place the MX Series router in configuration mode.

```
user@host# configure
```

3. On the MBG1 gateway, place the APN named Central in maintenance mode.

```
user@host# set unified-edge gateways ggsn-pgw MBG1 apn-services apns Central  
service-mode maintenance
```

4. Commit maintenance mode.

```
user@host# commit
```

5. Verify that the APN profile is in active maintenance mode where configuration changes are accepted for this object and all of its subhierarchies.

```
user@host# run show unified-edge ggsn-pgw MBG1 apn-services apns Central  
service-mode
```

```
Gateway Name   : MBG1
```

```
...
```

```
Profile Name   : Service Mode
```

```
Central        : Maintenance - Active Phase
```

6. Commit your changes and exit maintenance mode.

```
user@host# delete unified-edge gateways ggsn-pgw MBG1 apn-service apns Central  
service-mode  
user@host# commit
```

7. Return the gateway to operational state.

```
user@host# run show unified-edge ggsn-pgw gateway service-mode
```

**Results** The APN profile is placed in active maintenance mode. You can change profile attributes and commit them.

**Related Documentation**

- [Mobility Maintenance Mode Overview on page 592](#)
- [Modifying an Access Point Name on page 596](#)

---

## Example: Deleting an APN

---

- [Requirements on page 620](#)
- [Overview on page 621](#)
- [Configuration on page 621](#)

### Requirements

This example uses the following hardware and software components:

- An operational MX Series chassis
- Junos OS MobileNext Broadband Gateway package

## Overview

This configuration example shows how to delete an access point name (APN).

## Configuration

### Step-by-Step Procedure

To delete an APN:

1. Enter configuration mode and place the APN named Central in maintenance mode.

```
user@host# configure
user@host# set unified-edge gateways ggsn-pgw MBG1 apn-service apns Central
service-mode maintenance
user@host# commit
```

2. Wait for all sessions using Central to terminate. Do this by monitoring the service-mode status using the following show command. When sessions become zero, the service-mode status displays Maintenance – Active Phase.

```
user@host# run show unified-edge ggsn-pgw subscribers | match apn-name
```



**NOTE:** When maintenance mode shows Maintenance – Active Phase, the system is ready to accept configuration changes for all attributes of this object and its subhierarchies. When maintenance mode shows In/Out Phase, the system is ready to accept configuration changes only for non-maintenance mode attributes of this object and its subhierarchies.

3. Delete the APN named Central and commit the changes.

```
user@host# delete unified-edge ggsn-pgw MBG1 apn-services apnsCentral
user@host# commit
```

4. Exit maintenance mode and commit.

```
user@host# delete unified-edge ggsn-pgw MBG1 apn-services apns Central
service-mode
user@host# commit
```

5. Verify that the APN has been deleted.

```
user@host# run show configuration unified-edge gateways ggsn-pgw MBG1
apn-services apns
```

The APN named Central should not be displayed in the show command output.

6. Return the gateway to operational state.

```
user@host# run show unified-edge ggsn-pgw gateway service-mode
```

### Related Documentation

- [Mobility Maintenance Mode Overview on page 592](#)
- [Deleting an Access Point Name on page 599](#)

## Example: Changing a Charging Profile

---

This example shows how to change a charging profile using maintenance mode.

- [Requirements on page 622](#)
- [Overview on page 622](#)
- [Configuration on page 622](#)

### Requirements

This example uses the following hardware and software components:

- An installed and operational MX Series chassis
- Junos OS MobileNext Broadband Gateway package

### Overview

This configuration example shows how to place the charging profile named *juniper* in maintenance mode. Once in maintenance mode, you can make changes to the charging profile attributes without affecting mobility subscribers using other charging profiles.

You can modify the following attributes of a charging profile only when the charging profile is in maintenance mode:

- CDR profile
- Charging profile identifier (ID)
- Transport profile
- Trigger profile

### Configuration

#### Step-by-Step Procedure

To change a charging profile:

1. Verify the current status of maintenance mode for this charging profile.  

```
user@host> show unified-edge ggsn-pgw charging service-mode gateway MBG1
charging-profile juniper detail
```

```
Gateway Name   : MBG1
...
Profile Name   : juniper
Service Mode   : Operational
```
2. Place the broadband gateway in configuration mode.  

```
user@host# configure
```
3. On the gateway MBG1, place the charging profile named *juniper* in maintenance mode.

```
user@host# set unified-edge gateways ggsn-pgw MBG1 charging charging-profiles
juniper service-mode maintenance
```

4. Commit maintenance mode.

```
user@host# commit
```

5. Verify that the charging profile is in active maintenance mode where configuration changes will be accepted for this object and all of its subhierarchies.

```
user@host# run show unified-edge ggsn-pgw charging service-mode gateway MBG1
charging-profile juniper detail
```

```
Gateway Name : MBG1
```

```
...
```

```
Profile Name : Service Mode
```

```
juniper : Maintenance - Active Phase
```

6. Verify that there are no active subscribers using the charging profile.

```
user@host# run show unified-edge ggsn-pgw subscribers charging gateway MBG1
charging-profile juniper
```

7. (Optional) Use the **clear** command to terminate subscribers using the charging profile.

```
user@host# run clear unified-edge ggsn-pgw subscribers charging gateway MBG1
charging-profile juniper
```

When the subscriber count is zero and all sessions have ended, you can make and commit changes to the charging profile in active maintenance mode.

8. Modify the charging profile as required.



**NOTE:** These modifications must be made in active maintenance mode or they will fail.

9. Commit the changes and verify that they are properly committed.

```
user@host# commit
```

```
user@host# show unified-edge ggsn-pgw MBG1 charging charging-profile juniper
```

10. Exit maintenance mode and commit.

```
user@host# delete unified-edge gateways ggsn-pgw charging service-mode gateway
MBG1 charging-profile juniper service-mode
user@host# commit
```

**Results** The modified charging profile is effective for all subscribers who connect the gateway and who are linked to the charging profile.

#### Related Documentation

- [Changing a Charging Profile on page 601](#)
- [Deleting a Charging Profile on page 605](#)
- [Mobility Maintenance Mode Overview on page 592](#)

## Example: Changing a Transport Profile

---

This example shows how to change a transport profile using maintenance mode.

- [Requirements on page 624](#)
- [Overview on page 624](#)
- [Configuration on page 624](#)

### Requirements

This example uses the following hardware and software components:

- An installed and operational MX Series chassis
- Junos OS MobileNext Broadband Gateway package

### Overview

This configuration example shows how to put the transport profile “trans\_p” in maintenance mode. Once in maintenance mode, you can make changes to the transport profile attributes without affecting mobility subscribers using other transport profiles. You can modify the following attribute of a transport profile only when the transport profile is in maintenance mode:

- **cdr-release**

### Configuration

#### Step-by-Step Procedure

To modify a transport profile:

1. Verify the current status of maintenance mode for this transport profile.  

```
user@host> show unified-edge ggsn-pgw charging service-mode gateway MBG1
transport-profile trans_p detail
```

```
Gateway Name   : MBG1
...
Profile Name   : trans_p
Service Mode   : Operational
```
2. Set the broadband gateway in configuration mode.  

```
user@host# configure
```
3. On the gateway MBG1, place the transport profile “trans\_p” in maintenance mode.  

```
user@host# set unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
trans_p service-mode maintenance
```
4. Commit maintenance mode.  

```
user@host# commit
```
5. Verify that the transport profile is in active maintenance mode where configuration changes will be accepted for this object and all of its subhierarchies.

```
user@host# run show unified-edge ggsn-pgw charging service-mode gateway MBG1
transport-profile trans_p brief
```

```
Gateway Name   : MBG1
```

```
...
```

```
Profile Name   : Service Mode
```

```
trans_p       : Maintenance - Active Phase
```

6. Verify that there are no active subscribers using the transport profile.

```
user@host# run show unified-edge ggsn-pgw subscribers charging gateway MBG1
transport-profile trans_p
```

7. (Optional) Use the **clear** command to terminate subscribers using the transport profile.

```
user@host# run clear unified-edge ggsn-pgw subscribers charging gateway MBG1
transport-profile trans_p
```

When the subscriber count is zero and all sessions have ended, you can make and commit changes to the transport profile in active maintenance mode.

8. Modify the transport profile as required.



**NOTE:** These modifications must be made in active maintenance mode or they will fail.

9. Commit the changes and verify that they are properly committed.

```
user@host# commit
```

```
user@host# show unified-edge ggsn-pgw MBG1 charging transport-profile trans_p
```

10. Exit maintenance mode and commit.

```
user@host# delete unified-edge gateways ggsn-pgw charging service-mode gateway
MBG1 transport-profile trans_p service-mode
user@host# commit
```

**Results** The modified transport profile is effective for all subscribers who connect the gateway and who are linked to the transport profile.

#### Related Documentation

- [Changing a Transport Profile on page 603](#)
- [Deleting a Transport Profile on page 606](#)
- [Mobility Maintenance Mode Overview on page 592](#)

## Example: Changing Mobility Pool Attributes

- [Requirements on page 626](#)
- [Overview on page 626](#)
- [Configuration on page 626](#)

## Requirements

This example uses the following hardware and software components:

- An operational MX Series chassis
- Junos OS MobileNext Broadband Gateway package

## Overview

This example shows how to change mobility pool attributes for a mobile pool named “juniper-pool” in a routing instance named “default.”

## Configuration

### Step-by-Step Procedure

To change the address range for a mobility pool.

1. Verify the current configuration of the mobility pool.

```
user@host# run show configuration access address-assignment mobile-pools
juniper-pool {
  family inet {
    network {
      30.30.0.0/16 {
        range {
          range1 {
            low 30.30.1.1;
            high 30.30.255.254;
          }
        }
      }
    }
  }
  default-pool;
}
```

2. Enter configuration mode and then maintenance mode.

```
user@host# configure
user@host# set access address-assignment mobile-pools juniper-pool service-mode
maintenance
user@host# commit
```

3. Wait for all sessions using juniper-pool to terminate. Do this by monitoring the service-mode status using the following show command. When the number of sessions becomes zero, the service-mode status displays “Maintenance – Active Phase.”

```
user@host# show access address-assignment mobile-pools pool-name
service-mode
```





**NOTE:** “Maintenance - Active Phase” means system is ready to accept configuration changes for all attributes of this object and its subhierarchies. “Maintenance mode - In/Out Phase” means that the system is ready to accept configuration changes only for non-maintenance mode attributes of this object and its subhierarchies.

4. Change the address range from 30.30.x.x to 30.31.x.x.

```
user@host# configure
user@host# set access address-assignment mobile-pools juniper-pool family inet
network 30.31.0.0/16 range range1 low 30.31.1.1 high 30.31.255.254
user@host# configure
user@host# delete access address-assignment mobile-pools juniper-pool family
inet network 30.30.0.0/16
user@host# configure
user@host# commit
```

5. Check the state of this pool.

```
user@host# run show unified-edge ggsn-pgw address-assignment pool name
juniper-pool detail
```

6. Change the pool service mode to operational. Do this by deleting service-mode maintenance for juniper-pool.

```
user@host# configure
user@host# delete access address-assignment mobile-pools juniper-pool
service-mode maintenance
user@host# commit
```

7. Check the state of juniper-pool.

```
user@host# run show unified-edge ggsn-pgw address-assignment pool juniper-pool
details
```

8. Check the new configuration for juniper-pool.

```
user@host# run show configuration access address-assignment mobile-pools
juniper-pool
juniper-pool {
  family inet {
    network {
      30.31.0.0/16 {
        range {
          range1 {
            low 30.31.1.1;
            high 30.31.255.254;
          }
        }
      }
    }
  }
}
default-pool;
```

**Step-by-Step Procedure** The following examples illustrate how to make changes to mobile pools.

1. Verify the current configuration of "Gi-vrf".

```
user@host# run show routing-instances Gi-vrf access
```

```
address-assignment {
  mobile-pools {
    v4-vrf-1 {
      family inet {
        network {
          30.30.0.0/16 {
            range {
              range1 {
                low 30.30.1.1;
                high 30.30.254.254;
              }
            }
          }
        }
      }
    }
    v6-vrf-1 {
      family inet6 {
        network {
          2000:1:2::0/48 {
            range {
              range6-1 {
                low 2000:1:2:5::0/64;
                high 2000:1:2:ffff::0/64;
              }
            }
          }
        }
      }
    }
  }
}
```

2. Enter maintenance mode to make changes to *v4-vrf-1*. In this example, you are changing the range for the pool.

```
user@host# set routing-instances Gi-vrf access address-assignment mobile-pools
v4-vrf-1 service-mode maintenance
user@host# commit
user@host# set routing-instances Gi-vrf access address-assignment mobile-pools
v4-vrf-1 family inet network 30.30.0.0/16 range range1 low 30.30.2.1
user@host# commit
user@host# delete routing-instances Gi-vrf access address-assignment mobile-pools
v4-vrf-1 service-mode
user@host# commit
```

3. Verify your changes.

```
user@host# show routing-instances Gi-vrf access
```

```
address-assignment {
```

```

mobile-pools {
  v4-vrf-1 {
    family inet {
      network {
        30.30.0.0/16 {
          range {
            range1 {
              low 30.30.2.1;
              high 30.30.254.254;
            }
          }
        }
      }
    }
  }
  v6-vrf-1 {
    family inet6 {
      network {
        2000:1:2::0/48 {
          range {
            range6-1 {
              low 2000:1:2:5::0/64;
              high 2000:1:2:ffff::0/64;
            }
          }
        }
      }
    }
  }
}

[edit]
user@host#

```

**Step-by-Step Procedure** This procedure describes how to add a network to a mobile pool.

1. Verify the current address assignment for the mobile pool “jnpr”.

```
user@host# run show access address-assignment mobile-pools jnpr
```

```

family inet {
  network {
    30.30.0.0/16 {
      range {
        r1 {
          low 30.30.1.1;
          high 30.30.1.254;
        }
      }
    }
  }
}
default-pool;

```

2. Place the mobile pool in maintenance mode.

```
user@host# set access address-assignment mobile-pools jnpr service-mode
maintenance
user@host# commit
```

3. Verify that the pool is in maintenance mode.

```
user@host# show access address-assignment mobile-pools jnpr
```

```
service-mode maintenance;
family inet {
  network {
    30.30.0.0/16 {
      range {
        r1 {
          low 30.30.1.1;
          high 30.30.1.254;
        }
      }
    }
  }
}
default-pool;
```

4. Add the network “10.10.0.0/16”.

```
user@host# set access address-assignment mobile-pools jnpr family inet network
40.40.0.0/16
user@host# commit
```

5. Verify that the network was added to the pool.

```
user@host# run show access address-assignment mobile-pools jnpr
```

```
service-mode maintenance;
family inet {
  network {
    30.30.0.0/16 {
      range {
        r1 {
          low 30.30.1.1;
          high 30.30.1.254;
        }
      }
    }
    10.10.0.0/16; <----
  }
}
default-pool;
```

6. Exit maintenance mode and commit.

```
user@host# delete access address-assignment mobile-pools jnpr service-mode
user@host# commit
```

7. Verify that the pool is no longer in maintenance mode.

```
user@host# run show access address-assignment mobile-pools jnpr
```

```
family inet {
```

```

network {
  30.30.0.0/16 {
    range {
      r1 {
        low 30.30.1.1;
        high 30.30.1.254;
      }
    }
  }
  10.10.0.0/16; <----
}
default-pool;

```

8. Return the gateway to operational state.

```
user@host# run show unified-edge ggsn-pgw gateway service-mode
```

#### Related Documentation

- [Mobility Maintenance Mode Overview on page 592](#)
- [Changing Address Attributes in the Mobile Address Pool on page 607](#)

## Example: Deleting a Mobility Address Pool

- [Requirements on page 631](#)
- [Example of Deleting a Mobility Address Pool on page 631](#)
- [Configuration on page 632](#)

### Requirements

This example uses the following hardware and software components:

- An operational MX Series chassis
- Junos OS MobileNext Broadband Gateway package

### Example of Deleting a Mobility Address Pool

In this example, a pool “juniper-pool” in routing-instance “default” exists with the following configuration:

```

juniper-pool {
  family inet {
    network {
      30.30.0.0/16 {
        range {
          range1 {
            low 30.30.1.1;
            high 30.30.255.254;
          }
        }
      }
    }
  }
}

```

```
}  
default-pool;  
}
```

In this example, you delete this pool.

## Configuration

### Step-by-Step Procedure

To delete the pool, execute the following steps.

1. Enter configuration mode and place the pool in maintenance mode.

```
user@host# configure  
user@host# set access address-assignment mobile-pools juniper-pool service-mode  
maintenance  
user@host# commit
```

2. Wait for all sessions using “juniper-pool” to terminate. Do this by monitoring the service-mode status using the show command. When sessions become zero, the service-mode status will display Maintenance – Active Phase.

```
user@host# run show unified-edge ggsn-pgw address-assignment service-mode  
pool juniper-pool
```



**NOTE:** When maintenance mode shows “Maintenance – Active Phase,” the system is ready to accept configuration changes for all attributes of this object and its subhierarchies. When maintenance mode shows “In/Out Phase,” the system is ready to accept configuration changes only for non-maintenance mode attributes of this object and its subhierarchies.

3. Remove all references to the pool from all APNs, if any.

```
user@host# delete unified-edge gateways ggsn-pgw MBG1 apn-services apn internet  
address-assignment inet-pool pool juniper-pool  
user@host# commit
```

4. Remove all references to the pool from any pool group, if any.

```
user@host# delete access address-assignment mobile-pool-groups pool-group-xyz  
juniper-pool  
user@host# commit
```

5. If the pool is marked default pool, many APNs could be referencing this pool. In this case, delete the default pool attribute for the “juniper-pool.”

```
user@host# delete access address-assignment mobile-pools juniper-pool  
default-pool  
user@host# commit
```

6. Delete the pool “juniper-pool.”

```
user@host# delete access address-assignment mobile-pools juniper-pool  
routing-instance juniper-vrf  
user@host# commit
```

7. Verify that the address pool is deleted.

```
user@host# run show unified-edge ggsn-pgw address-assignment pool details
```

The address pool “juniper-pool” should not be displayed in the show command output.

#### Related Documentation

- [Mobility Maintenance Mode Overview on page 592](#)
- [Deleting a Mobile Address Pool on page 609](#)

## Example: Modifying Mobile Interface Parameters

- [Requirements on page 633](#)
- [Overview on page 633](#)
- [Configuration on page 633](#)

### Requirements

This example uses the following hardware and software components:

- An operational MX Series chassis
- Junos OS MobileNext Broadband Gateway package

### Overview

The following examples show how to make changes to a mobile interface.

### Configuration

Use the following examples to change to a mobile interface:

- [Modifying the IPv4 Maximum Transmission Unit \(MTU\) on page 633](#)
- [Changing the Mobile Interface for an Access Point Name \(APN\) on page 634](#)

#### Modifying the IPv4 Maximum Transmission Unit (MTU)

#### Step-by-Step Procedure

The following procedure shows how to modify the IPv4 maximum transmission unit (MTU).

1. Set the MX Series router in configuration mode.  

```
user@host# configure
```
2. On the *MBG1* gateway, place the APN *alice1* in maintenance mode.  

```
user@host# set unified-edge gateways ggsn-pgw MBG1 apn-services apn alice1 service-mode maintenance
```
3. Commit maintenance mode.  

```
user@host# commit
```
4. Verify that the APN is in active maintenance mode where configuration changes will be accepted for this object and all of its subhierarchies.

```
user@host# run show unified-edge ggsn-pgw apn service-mode apn alice1
maintenance mode
```

```
APN Name      : Service Mode
alice1        : Maintenance - Active Phase
```

5. Change and commit the MTU to 1550.

```
user@host# set interfaces mif unit 2 family inet mtu 1550
user@host# commit
```

6. Commit your changes and exit maintenance mode.

```
user@host# delete unified-edge gateways ggsn-pgw MBG1 apn-services apn alice1
service-mode
user@host# commit
```

7. Verify that the change has been made.

```
user@host# show interfaces mif.2

Logical interface mif.2 (Index 719) (SNMP ifIndex 771)
Flags: SNMP-Traps Encapsulation: GTP-over-MIF
Bandwidth: 1000mbps
Input packets : 0
Output packets: 0
Protocol inet, MTU: 1550
  Flags: Sendbcst-pkt-to-re, User-MTU
Protocol inet6, MTU: 1600
  Addresses, Flags: Is-Preferred
    Destination: fe80::/64, Local: fe80::2a0:a5ff:fc67:587b
```

8. Return the gateway to operational state.

```
user@host# run show unified-edge ggsn-pgw gateway service-mode
```

---

### Changing the Mobile Interface for an Access Point Name (APN)

---

**Step-by-Step Procedure** This procedure describes how to change the mobile interface for the APN casper from .0 to 222.

1. Verify the state of *casper*.

```
user@host# run show unified-edge ggsn-pgw apn service-mode
```

#### Maintenance Mode

MM Active Phase - System is ready to accept configuration changes for all attributes of this object and its sub-hierarchies.

MM In/Out Phase - System is ready to accept configuration changes only for non-maintenance mode attributes of this object and its sub-hierarchies.

APN Name	Service Mode
apn-vrf1.juniper.net	Operational
apn-vrf2.juniper.net	Operational
apn-vrf3.juniper.net	Operational
casper.com	Operational
fuzz-gtp	Operational



```

new-ipv4           Operational
new-ipv6           Operational
radius1            Operational
realapn1           Operational
static-assign      Operational
virtual-apn3.juniper.net Operational
virtualapn.juniper.net Operational
virtualapn2.juniper.net Operational

```

```

[edit]
user@host#

```

2. Place the APN *casper.com* in maintenance mode.

```

user@host# set unified-edge gateways ggsn-pgw PGW apn-services apn casper.com
service-mode maintenance
user@host# commit

```

3. Change the mobile interface.

```

user@host# set unified-edge gateways ggsn-pgw PGW apn-services apn casper.com
mobile-interface mif.222
user@host# commit

```

4. Verify the change.

```

user@host# run show unified-edge gateways ggsn-pgw PGW apn-services apn
casper.com

```

```

apn-type real;
apn-data-type ipv4v6;
mobile-interface mif.222;
address-assignment {
    local;
}
user-options {
    use-apnname;
}
dns-server {
    primary-v4 4.4.4.1;
}
p-cscf {
    2001:1:4:3::;
}
selection-mode {
    from-ms;
    from-sgsn;
}
service-mode maintenance; <---- mode

```

```

[edit]
user@host#

```

5. Return the APN “casper” to normal operation (exit maintenance mode and commit your changes).

```

user@host# delete unified-edge gateways ggsn-pgw PGW apn-services apn
casper.com service-mode
user@host# commit

```

6. Return the gateway to operational state.

```
user@host# run show unified-edge ggsn-pgw gateway service-mode
```

**Related  
Documentation**

- [Mobility Maintenance Mode Overview on page 592](#)
- [Deleting a Mobile Address Pool on page 609](#)

---

## Example: Deleting a Session PIC

This example shows how to delete a session PIC using maintenance mode at the **[edit unified-edge gateways ggsn-pgw ggsn-pgw-name system session-pics interface]** or **[edit unified-edge gateways sgw sgw-name system session-pics interface]** hierarchy level. The session PIC can be an aggregated multiservices interface (AMS). Session PICs process control plane messages on a broadband gateway.

- [Requirements on page 636](#)
- [Overview on page 636](#)
- [Configuration on page 636](#)
- [Verification on page 639](#)
- [Troubleshooting Session PIC Deletion on page 639](#)

### Requirements

This example uses the following hardware and software components:

- An installed and operational MobileNext Broadband Gateway chassis
- Properly installed and operational Junos OS MobileNext Broadband Gateway software packages

Before you delete a session PIC using maintenance mode:

- Make sure that this change has been coordinated with affected groups and users.

### Overview

This configuration example shows how to put the session PIC interface in maintenance mode. Once in maintenance mode, you can delete the session PIC without affecting mobility subscribers using other session PICs.

---

#### Topology

This procedure is independent of other network devices.

### Configuration

To configure session PIC maintenance mode and deletion, perform this tasks:

- [Configuring Maintenance Mode for Session PIC Deletion on page 637](#)
- [Results on page 638](#)

**CLI Quick  
Configuration**

Delete session PIC **ms-1/1/0** from gateway **MBG1**:

```
[edit]
set unified-edge gateways ggsn-pgw MBG1 system session-pics interface ms-1/1/0
  service-mode maintenance
commit
delete unified-edge gateways ggsn-pgw MBG1 system interface ms-1/1/0
commit
```

### Configuring Maintenance Mode for Session PIC Deletion

---

**Step-by-Step  
Procedure**

To configure maintenance mode and session PIC deletion:

1. Verify the current status of maintenance mode for this session PIC.

```
user@MBG1> show unified-edge ggsn-pgw MBG1 system interfaces service-mode
```



**NOTE:** The **service-mode** option displays the information details about maintenance mode as well as status.

#### Maintenance Mode

MM Active Phase - System is ready to accept configuration changes for all attributes of this object and its sub-hierarchies.

MM In/Out Phase - System is ready to accept configuration changes only for non-maintenance mode attributes of this object and its sub-hierarchies.

Interface Name	Gateway Name	Service Mode
ms-1/0/0	MBG1	Operational
ms-1/1/0	MBG1	Operational
ms-2/0/0	MBG1	Operational
ms-2/1/0	MBG1	Operational
pfe-0/0/0	MBG1	Operational
pfe-0/1/0	MBG1	Operational
pfe-0/2/0	MBG1	Operational
pfe-0/3/0	MBG1	Operational
ams1	MBG1	Operational

2. Place the broadband gateway in configuration mode.

```
user@MBG1# configure
```

3. On the gateway **MBG1**, place the interface **ms-1/1/0** in maintenance mode.

```
user@MBG1# set unified-edge gateways ggsn-pgw MBG1 system session-pics
  interface ms-1/1/0 service-mode maintenance
```

4. Commit maintenance mode.

```
user@MBG1# commit
```

5. Verify that the session PIC is in active maintenance mode where configuration changes will be accepted for this object and all of its subhierarchies.

```
user@MBG1> show unified-edge ggsn-pgw MBG1 system interfaces service-mode
```

**Maintenance Mode**

MM Active Phase - System is ready to accept configuration changes for all attributes of this object and its sub-hierarchies.

MM In/Out Phase - System is ready to accept configuration changes only for non-maintenance mode attributes of this object and its sub-hierarchies.

Interface Name	Gateway Name	Service Mode
ms-1/0/0	MBG1	Operational
ms-1/1/0	MBG1	Maintenance - Active Phase
ms-2/0/0	MBG1	Operational
ms-2/1/0	MBG1	Operational
pfe-0/0/0	MBG1	Operational
pfe-0/1/0	MBG1	Operational
pfe-0/2/0	MBG1	Operational
pfe-0/3/0	MBG1	Operational
ams1	MBG1	Operational



**NOTE:** All subscribers serviced by the session PIC must go to zero. All Charging Data Records (CDRs) for these subscribers must be flushed out. You can wait for these conditions to be met, or use the clear command for the interface (or gateway) to force these conditions.

6. Delete the session PIC.

```
user@MBG1# delete unified-edge gateways ggsn-pgw MBG1 system interface  
ms-1/1/0
```

7. Exit maintenance mode and commit.



**NOTE:** Deletion of a session PIC automatically exits maintenance mode for the deleted PIC.

```
user@MBG1# commit
```

---

**Results**

The session PIC **ms-1/1/0** is removed from the gateway interface list.

```
user@MGB1> show unified-edge ggsn-pgw MBG1 system interfaces service-mode
```

**Maintenance Mode**

MM Active Phase - System is ready to accept configuration changes for all attributes of this object and its sub-hierarchies.

MM In/Out Phase - System is ready to accept configuration changes only for non-maintenance mode attributes of this object and its sub-hierarchies.

Interface Name	Gateway Name	Service Mode
----------------	--------------	--------------

```

ms-1/0/0 MBG1      Operational
ms-2/0/0 MBG1      Operational
ms-2/1/0 MBG1      Operational
pfe-0/0/0 MBG1     Operational
pfe-0/1/0 MBG1     Operational
pfe-0/2/0 MBG1     Operational
pfe-0/3/0 MBG1     Operational
ams1 MBG1          Operational

```

## Verification

- [Verifying Session PIC Deletion on page 639](#)

### Verifying Session PIC Deletion

**Purpose** To verify that the session PIC is no longer part of the gateway configuration.

**Action** Display the interfaces configured for the gateway.

```

user@MBG1> show unified-edge ggsn-pgw system interfaces
Gateway: MBG1
Interfaces Members Operational Redundancy
           State Role
ms-1/0/0   Active Standalone
ms-2/0/0   Active Standalone
ms-2/1/0   Active Standalone
pfe-0/0/0   Active Standalone
pfe-0/1/0   Active Standalone
pfe-0/2/0   Active Standalone
pfe-0/3/0   Active Standalone
ams1       Active Standalone

```



**NOTE:** The session PIC `ms-1/1/0` no longer appears on the list of gateway interfaces.

**Meaning** Deletion of session PIC successful.

## Troubleshooting Session PIC Deletion

To troubleshoot session PIC deletion with maintenance mode, perform this task:

- [Troubleshooting a Commit Fail on page 639](#)

### Troubleshooting a Commit Fail

**Problem** The final commit after deletion of the session PIC fails.

**Solution** The `ms-1/1/0` interface (FPC 1 and PIC 1) can still have the mobility package configured at the `[edit chassis]` hierarchy level. You must remove the `jservices-mobile` package from the session PIC configuration, then perform the commit.

- Related Documentation**
- [Mobility Maintenance Mode Overview on page 592](#)
  - [Deleting a Session PIC on page 610](#)

## Example: Deleting a Services PIC

---

This example shows how to delete a services PIC using maintenance mode at the **[edit unified-edge gateways ggsn-pgw *ggsn-pgw-name* system service-pics interface]** or **[edit unified-edge gateways sgw *sgw-name* system service-pics interface]** hierarchy level. The services PIC can be an aggregated multiservices interface (AMS). Services PICs perform packet-related services on a broadband gateway.

- [Requirements on page 640](#)
- [Overview on page 640](#)
- [Configuration on page 640](#)
- [Verification on page 643](#)

### Requirements

This example uses the following hardware and software components:

- An installed and operational MobileNext Broadband Gateway chassis
- Properly installed and operational Junos OS MobileNext Broadband Gateway software packages

Before you delete a services PIC using maintenance mode:

- Make sure that this change has been coordinated with affected groups and users

### Overview

This configuration example shows how to put the services PIC interface in maintenance mode. Once in maintenance mode, you can delete the services PIC without affecting mobility subscribers using other services PICs.

#### Topology

---

This procedure is independent of other network devices.

### Configuration

To configure services PIC maintenance mode and deletion, perform this task:

- [Configuring Maintenance Mode for Services PIC Deletion on page 641](#)
- [Results on page 642](#)

**CLI Quick Configuration**

Delete services PIC **ms-2/0/0** from gateway **MBG1**:

```
[edit]
set unified-edge gateways ggsn-pgw MBG1 system service-pics interface ms-2/0/0
service-mode maintenance
```

```
commit
delete unified-edge gateways ggsn-pgw MBG1 system interface ms-2/0/0
commit
```

### Configuring Maintenance Mode for Services PIC Deletion

#### Step-by-Step Procedure

To configure maintenance mode for services PIC deletion:

1. Verify the current status of maintenance mode for this services PIC.

```
user@MBG1> show unified-edge ggsn-pgw MBG1 system interfaces service-mode
```



**NOTE:** The `service-mode` option displays the information details about maintenance mode as well as status.

#### Maintenance Mode

MM Active Phase - System is ready to accept configuration changes for all attributes of this object and its sub-hierarchies.

MM In/Out Phase - System is ready to accept configuration changes only for non-maintenance mode attributes of this object and its sub-hierarchies.

```
Interface Name Gateway Name Service Mode
ms-1/0/0 MBG1 Operational
ms-1/1/0 MBG1 Operational
ms-2/0/0 MBG1 Operational
ms-2/1/0 MBG1 Operational
pfe-0/0/0 MBG1 Operational
pfe-0/1/0 MBG1 Operational
pfe-0/2/0 MBG1 Operational
pfe-0/3/0 MBG1 Operational
ams1 MBG1 Operational
```

2. Place the broadband gateway in configuration mode.

```
user@MBG1# configure
```

3. On the gateway MBG1, place the interface `ms-2/0/0` in maintenance mode.

```
user@MBG1# set unified-edge gateways ggsn-pgw MBG1 system service-pics
interface ms-2/0/0 service-mode maintenance
```

4. Commit maintenance mode.

```
user@MBG1# commit
```

5. Verify that the services PIC is in active maintenance mode where configuration changes will be accepted for this object and all of its subhierarchies.

```
user@MBG1> show unified-edge ggsn-pgw MBG1 system interfaces service-mode
```

#### Maintenance Mode

MM Active Phase - System is ready to accept configuration changes for all attributes of this object and its sub-hierarchies.

MM In/Out Phase - System is ready to accept configuration changes only for non-maintenance mode attributes of this object and its sub-hierarchies.

Interface Name	Gateway Name	Service Mode
ms-1/0/0	MBG1	Operational
ms-1/1/0	MBG1	Operational
ms-2/0/0	MBG1	Maintenance - Active Phase
ms-2/1/0	MBG1	Operational
pfe-0/0/0	MBG1	Operational
pfe-0/1/0	MBG1	Operational
pfe-0/2/0	MBG1	Operational
pfe-0/3/0	MBG1	Operational
ams1	MBG1	Operational



**NOTE:** All subscribers serviced by the services PIC must go to zero. All Charging Data Records (CDRs) for these subscribers must be flushed out. You can wait for these conditions to be met, or use the `clear` command for the interface (or gateway) to force these conditions.

6. Delete the services PIC.

```
user@MBG1# delete unified-edge gateways ggsn-pgw MBG1 system interface
ms-2/0/0
```

7. Exit maintenance mode and commit.



**NOTE:** Deletion of a services PIC automatically exits maintenance mode for the deleted PIC.

```
user@MBG1# commit
```

---

## Results

The services PIC `ms-2/0/0` is removed from the gateway interface list.

```
user@MGB1> show unified-edge ggsn-pgw MBG1 system interfaces service-mode
```

### Maintenance Mode

MM Active Phase - System is ready to accept configuration changes for all attributes of this object and its sub-hierarchies.

MM In/Out Phase - System is ready to accept configuration changes only for non-maintenance mode attributes of this object and its sub-hierarchies.

Interface Name	Gateway Name	Service Mode
ms-1/0/0	MBG1	Operational
ms-1/1/0	MBG1	Operational
ms-2/1/0	MBG1	Operational
pfe-0/0/0	MBG1	Operational



```

pfe-0/1/0 MBG1      Operational
pfe-0/2/0 MBG1      Operational
pfe-0/3/0 MBG1      Operational
ams1 MBG1 Operational

```

## Verification

- [Verifying Services PIC Deletion on page 643](#)

### Verifying Services PIC Deletion

**Purpose** To verify that the services PIC is no longer part of the gateway configuration.

**Action** Display the interfaces configured for the gateway.

```

user@MBG1> show unified-edge ggsn-pgw system interfaces
Gateway: MBG1
Interfaces Members Operational Redundancy
          State      Role
ms-1/0/0      Active   Standalone
ms-2/0/0      Active   Standalone
ms-2/1/0      Active   Standalone
pfe-0/0/0     Active   Standalone
pfe-0/1/0     Active   Standalone
pfe-0/2/0     Active   Standalone
pfe-0/3/0     Active   Standalone
ams1          Active   Standalone

```



**NOTE:** The services PIC ms-2/0/0 no longer appears on the list of gateway interfaces.

**Meaning** Deletion of services PIC successful.

**Related Documentation**

- [Mobility Maintenance Mode Overview on page 592](#)
- [Deleting a Services PIC on page 612](#)

## Example: Changing an AMS Interface

This example shows how to change the parameters for an aggregated multiservices (AMS) interface on a MobileNext Broadband Gateway using maintenance mode at the **[edit interfaces]** hierarchy level. If an AMS interface is configured under a gateway's session PICs or services PICs, and there is a change to any load-balancing options such as membership of AMS interfaces (**mams-**), then the AMS interface must be in maintenance mode.

- [Requirements on page 644](#)
- [Overview on page 644](#)

- [Configuration on page 644](#)
- [Verification on page 647](#)

## Requirements

This example uses the following hardware and software components:

- An installed and operational MobileNext Broadband Gateway chassis
- Properly installed and operational Junos OS MobileNext Broadband Gateway software packages

Before you change AMS parameters using maintenance mode:

- Make sure that this change has been coordinated with affected groups and users.

## Overview

This configuration example shows how to put the AMS interface in maintenance mode. Once in maintenance mode, you can delete a member (mams-) of the AMS group, add another member, and change the preferred backup, all without affecting mobility subscribers.

---

### Topology

This procedure is independent of other network devices.

## Configuration

To configure AMS maintenance mode and parameter changes, perform this task:

- [Configuring Maintenance Mode for AMS Parameter Change on page 645](#)
- [Results on page 647](#)

**CLI Quick Configuration** Delete **mams-5/1/0** from **ams1**, add **mams-3/1/0** to **ams1**, and configure **mams-3/1/0** as the new preferred backup for **ams1**:

```
[edit]
set unified-edge ggsn-pgw gateway-name system interface ams1 service-mode
  maintenance
commit
delete unified-edge ggsn-pgw gateway-name system interface ams1 load-balancing-options
  member-interface mams-5/1/0
set interfaces ams1 load-balancing-options member-interface mams-3/1/0
delete interfaces ams1 load-balancing-options high-availability-options many-to-one
  preferred-backup mams-5/1/0
set interfaces ams1 load-balancing-options high-availability-options many-to-one
  preferred-backup mams-3/1/0
delete unified-edge ggsn-pgw gateway-name system interface ams1 service-mode
  maintenance
commit
```



**NOTE:** This example requires changes at both the [edit unified-edge] and [edit interfaces] hierarchy levels. In this example, the interface `ams1` is set as `anchor-services-pics` at the [edit unified-edge gateways ggsn-pgw MBG1 system] hierarchy level.

### Configuring Maintenance Mode for AMS Parameter Change

#### Step-by-Step Procedure

To configure maintenance mode and AMS parameter change:

1. Verify the current status of maintenance mode for this AMS (`ams1`).

```
user@MBG1> show unified-edge ggsn-pgw MBG1 system interfaces service-mode
```



**NOTE:** The `service-mode` option displays the information details about maintenance mode as well as status.

#### Maintenance Mode

MM Active Phase - System is ready to accept configuration changes for all attributes of this object and its sub-hierarchies.

MM In/Out Phase - System is ready to accept configuration changes only for non-maintenance mode attributes of this object and its sub-hierarchies.

```
Interface Name Gateway Name Service Mode
ms-1/0/0 MBG1 Operational
ms-1/1/0 MBG1 Operational
ms-2/0/0 MBG1 Operational
ms-2/1/0 MBG1 Operational
pfe-0/0/0 MBG1 Operational
pfe-0/1/0 MBG1 Operational
pfe-0/2/0 MBG1 Operational
pfe-0/3/0 MBG1 Operational
ams1 MBG1 Operational
```

2. Place the broadband gateway in configuration mode.

```
user@MBG1# configure
```

3. Show the current configuration for `ams1`

```
user@MBG1# show unified-edge ggsn-pgw gateway-name system interface ams1
load-balancing-options {
  member-interface mams-4/1/0;
  member-interface mams-5/1/0;
  member-failure-options {
    redistribute-all-traffic {
      enable-rejoin;
    }
  }
  high-availability-options {
```

```

        many-to-one {
            preferred-backup mams-5/1/0;
        }
    }
    unit 1 {
        family inet;
    }
    unit 2 {
        family inet;
    }

```

4. On the gateway MBG1, place the interface **ams1** in maintenance mode.

```

user@MBG1# set unified-edge ggsn-pgw gateway-name system interface ams1
service-mode maintenance

```

5. Commit maintenance mode.

```

user@MBG1# commit

```

6. Verify that the **ams1** interface is in active maintenance mode where configuration changes will be accepted for this object and all of its subhierarchies.

```

user@MGB1> show unified-edge ggsn-pgw MBG1 system interfaces service-mode

```

#### Maintenance Mode

MM Active Phase - System is ready to accept configuration changes for all attributes of this object and its sub-hierarchies.

MM In/Out Phase - System is ready to accept configuration changes only for non-maintenance mode attributes of this object and its sub-hierarchies.

#### Interface Name Gateway Name Service Mode

```

ms-1/0/0 MBG1 Operational
ms-1/1/0 MBG1 Operational
ms-2/0/0 MBG1 Operational
ms-2/1/0 MBG1 Operational
pfe-0/0/0 MBG1 Operational
pfe-0/1/0 MBG1 Operational
pfe-0/2/0 MBG1 Operational
pfe-0/3/0 MBG1 Operational
ams1 MBG1 Maintenance - Active Phase

```



**NOTE:** All subscribers serviced by **ams1** must go to zero. All Charging Data Records (CDRs) for these subscribers must be flushed out. You can wait for these conditions to be met, or use the **clear** command for the interface (or gateway) to force these conditions.

7. Delete the **mams-5/1/0** member interface for **ams1**.

```

user@MBG1# delete unified-edge ggsn-pgw gateway-name system interface ams1
load-balancing-options member-interface mams-5/1/0

```

8. Add the **mams-3/1/0** member interface for **ams1** at the **[edit interfaces]** hierarchy level.

```
user@MBG1# set interfaces ams1 load-balancing-options member-interface
mams-3/1/0
```

9. Delete the **mams-5/1/0** member interface as the preferred backup for **ams1** at the **[edit interfaces]** hierarchy level.

```
user@MBG1# delete interfaces ams1 load-balancing-options high-availability-options
many-to-one preferred-backup mams-5/1/0
```

10. Add the **mams-3/1/0** member interface as the preferred backup for **ams1** at the **[edit interfaces]** hierarchy level.

```
user@MBG1# set interfaces ams1 load-balancing-options high-availability-options
many-to-one preferred-backup mams-3/1/0
```

11. Exit maintenance mode and commit.

```
user@MBG1# delete unified-edge ggsn-pgw gateway-name system interface ams1
service-mode maintenance
user@MBG1# commit
```

## Results

The parameters for **ams1** are changed, so that **mams-3/1/0** has replaced **mams-5/1/0** as a member interface and preferred backup.

```
user@MBG1# show unified-edge ggsn-pgw gateway-name system interfaces ams1
load-balancing-options {
  member-interface mams-3/1/0;
  member-interface mams-4/1/0;
  member-failure-options {
    redistribute-all-traffic {
      enable-rejoin;
    }
  }
  high-availability-options {
    many-to-one {
      preferred-backup mams-3/1/0;
    }
  }
}
unit 1 {
  family inet;
}
unit 2 {
  family inet;
}
```

## Verification

- [Verifying AMS parameter change on page 648](#)

### Verifying AMS parameter change

---

**Purpose** To verify that the members of **ams1** have changed.

**Action** Display the interfaces configured for **ams1**.

```
user@MBG1> show unified-edge ggsn-pgw gateway-name system interfaces load-balancing ams1
```

```
Load-balancing interfaces detail
```

```
Interface   : ams1
```

```
State       : Up
```

```
Last change  : 00:11:28
```

```
Member count : 2
```

```
HA Model    : Many-to-One
```

```
Members     :
```

```
  Interface  Weight State
```

```
  mams-4/1/0  10  Active
```

```
  mams-3/1/0  10  Backup
```

```
Sync-state  :
```

```
  Interface  Status
```

```
  mams-3/1/0  Unknown
```

```
  mams-4/1/0  Unknown
```

**Meaning** The parameters for **ams1** have successfully changed.

- Related Documentation**
- [Mobility Maintenance Mode Overview on page 592](#)
  - [Changing AMS Interface Parameters on page 614](#)
  - [Changing Gateway Parameters with Maintenance Mode on page 617](#)

## PART 11

# Configuration Examples

- [Mobility Configuration Examples on page 651](#)





# Mobility Configuration Examples

- [Example: Simple Unified Edge Configuration on page 651](#)
- [Example: Configuring MobileNext Broadband Gateway on page 658](#)
- [Example: Configuring MobileNext Broadband Gateway with Provider Edge Functionality on page 689](#)
- [Example: Configuring NAT on page 698](#)
- [Example: Configuring a Standalone S-GW on page 702](#)
- [Example: Configuring a Collocated P-GW and S-GW on page 708](#)
- [Example: Configuring a Multigateway P-GW and S-GW on page 719](#)

## Example: Simple Unified Edge Configuration

---

This example describes how to configure a simple unified edge, and consists of the following sections:

- [Requirements on page 651](#)
- [Overview and Topology on page 651](#)
- [Configuration on page 652](#)
- [Verification on page 657](#)

### Requirements

This example requires the following hardware and software:

- Hardware — MX240, MX480, or MX960 with MOB-MS-DPC
- Software — Junos OS Release 11.2W or later

### Overview and Topology

This example includes the following components:

- SGSN (serving GPRS support node) — The SGSN is the gateway between the mobile user equipment and the core network in a GPRS/UMTS network. Signaling to or from this node is processed on interface ge-2/1/1.

- GGSN (gateway GPRS support node)—The GGSN is responsible for interaction between the GPRS network and external packet-switched networks, such as the Internet. For the external network, the GGSN functions like a router to a subnetwork. The GGSN hides the GPRS infrastructure from the external network. The GGSN is the anchor point that enables the mobility of the user terminal in the GPRS/UMTS network. Its function in GPRS is similar to the home agent in Mobile IP. It maintains the routing necessary to tunnel the protocol data units (PDUs) to the SGSN that services a particular mobile station (MS). It also performs authentication, charging functions, QoS, and policy enforcement.
- Connectivity from the user equipment to external packet data networks

[Table 60 on page 652](#) shows the MobileNext Broadband Gateway components used in this solution.

**Table 60: Unified Edge — Simple Configuration**

Component	Configuration	Settings
SGSN-facing interface	ge-2/1/1	200.6.1.1/24
GGSN	unified-edge ggsn-pgw gateway PGW	<b>gn interface lo0.0 v4-address 99.1.1.1</b> Loopback interface for receiving packets from the Packet Forwarding Engine.
Mobility control plane	ms-3/0/0	Services PIC used for processing packets received from the Packet Forwarding Engine.
Mobility control plane	ms-3/1/0	<b>unit 16000</b> —Unit required for outgoing packets.  <b>unit 0</b> —One unit required for each APN destination.
Mobile address assignment pool	default-ipv4-address-pool	<b>network 29.0.0.0/8</b> —Subnet for address assignment to user equipment.  <b>range r1</b> —Named address range.  <b>low 29.0.0.1</b> —Lowest address available.  <b>high 29.255.255.254</b> —Highest address available.

## Configuration

To configure a simple unified edge environment, perform the following tasks:

- [Configuring the Hardware Components for Mobility on page 653](#)
- [Configuring the Interface to the Gn Side on page 654](#)

- [Configuring the Mobile Interface Units for Mobility Support on page 654](#)
- [Configuring the Address Pool for Assigning IP Addresses to the User Equipment on page 655](#)
- [Configuring the GGSN Parameters on page 656](#)

### Configuring the Hardware Components for Mobility

#### CLI Quick Configuration

To quickly configure the chassis for this example, copy the following commands and paste them into the router terminal window:

```
[edit]
load merge /etc/config/mobility-defaults.conf
set chassis fpc 2 forwarding-packages mobility ggsn-pgw
set chassis fpc 3 pic 0 apply-groups mobility
set chassis fpc 3 pic 1 apply-groups mobility
```

#### Step-by-Step Procedure

To configure the chassis options that support the unified edge:

1. Load and merge the default configuration file for the **mobility** group.

```
[edit]
user@host# load merge /etc/config/mobility-defaults.conf
```

2. Configure the forwarding package at the FPC level.

```
[edit]
user@host# set chassis fpc 2 forwarding-packages mobility ggsn-pgw
```



**NOTE:** You must include every Packet Forwarding Engine configured with the **ggsn-pgw** forwarding package at the **[edit unified-edge gateways ggsn-pgw gateway-name system anchor-pfes]** hierarchy level on the broadband gateway. If you do not specify the Packet Forwarding Engine as an anchor interface, then the Packet Forwarding Engine will not be used by the broadband gateway.

3. Configure the **mobility** group for the services PICs that are processing the packets.

```
[edit]
user@host# set chassis fpc 3 pic 0 apply-groups mobility
user@host# set chassis fpc 3 pic 1 apply-groups mobility
```



**NOTE:** You must include every services PIC configured with the **jservices-mobile** package at the **[edit unified-edge gateways ggsn-pgw gateway-name system anchor-spics]** hierarchy level on the broadband gateway. If you do not include the services PIC as an anchor interface, then the services PIC will not be used by the broadband gateway.

### Configuring the Interface to the Gn Side

---

**CLI Quick Configuration** To quickly configure the interface to the Gn side (SGW/SGSN signaling), copy the following commands and paste them into the router terminal window:

```
[edit interfaces ge-2/1/1]
set description sgw-em0
set unit 0 family inet address 200.6.1.1/24
```

**Step-by-Step Procedure** To configure the interface to the SGSN (signaling) function:

1. Identify the interface.  

```
user@host# edit interfaces ge-2/1/1
```
2. Provide a description that identifies the function of the interface.  

```
[edit interfaces ge-2/1/1]
user@host# set description sgw-em0
```
3. Identify the unit and IP address for the interface.  

```
[edit interfaces ge-2/1/1]
user@host# set unit 0 family inet address 200.6.1.1/24
```

**Results** Check the results of the configuration:

```
root@host> show configuration interfaces ge-2/1/1
description sgw-em0;
unit 0 {
  family inet {
    address 200.6.1.1/24;
  }
}
```

### Configuring the Mobile Interface Units for Mobility Support

---

**CLI Quick Configuration** To quickly configure the mobile interface units needed to process packets on the services PIC, copy the following commands and paste them into the router terminal window:

```
[edit interfaces mif]
edit interfaces mif
set unit 0 family inet
set unit 1 family inet
set unit 2 family inet
set unit 16000 family inet
```

**Step-by-Step Procedure** To configure the mobile interface units used to process information packets on the services PIC:

1. Access the mobile interface hierarchy.  

```
user@host# edit interfaces mif
```
2. Assign one mobile interface for each access point name.  

```
[edit interfaces mif]
user@host# edit interfaces mif
```

```

user@host# set unit 0 family inet
user@host# set unit 1 family inet
user@host# set unit 2 family inet
user@host# set unit 16000 family inet description "Reserved mobile interface"

```

**Results** Check the results of the configuration:

```

user@host# edit interfaces mif
user@host# show
unit 0 {
    family inet;
}
unit 1 {
    family inet;
}
unit 2 {
    family inet;
}
unit 16000 {
    description "Reserved mobile interface";
    family inet;
}

user@host# edit configuration interfaces ms-3/1/0
user@host# show
unit 16000 {
    family inet;
}

user@host# edit configuration interfaces mif
user@host# show
unit 0 {
    family inet;
}
unit 1 {
    family inet;
}
unit 16000 {
    family inet;
}

```

### Configuring the Address Pool for Assigning IP Addresses to the User Equipment

**CLI Quick Configuration** To quickly configure the address pool for assigning IP addresses to the user equipment, copy the following commands and paste them into the router terminal window:

```

[edit access address-assignment mobile-pools default-pool family inet network]
user@host# set 29.0.0.0/8 range r1 low 29.0.0.1 high 29.255.255.254

```

**Step-by-Step Procedure** To configure the address pool for assigning IP addresses to user equipment:

1. Create a named pool.
 

```

user@host# edit access address-assignment mobile-pools
default-ipv4-address-pool

```
2. Optionally, set the pool as the default pool.
 

```

[edit access address assignment mobile-pools default-ipv4-address-pool ]

```

```
user@host# set default-pool
```

3. Set the network address for the pool and a range of available addresses.

```
[edit access address assignment mobile-pools default-ipv4-address-pool]
user@host# set family inet network 29.0.0.0/8 range r1 low 29.0.0.1 high
29.255.255.254
```

**Results** Check the results of the configuration:

```
user@host# edit access
user@host# show
access {
  address-assignment {
    mobile-pools {
      default-ipv4-address-pool {
        family inet {
          network {
            29.0.0.0/8 {
              range {
                r1 {
                  low 29.0.0.1;
                  high 29.255.255.254;
                }
              }
            }
          }
        }
      }
    }
  }
}
```

---

### Configuring the GGSN Parameters

**CLI Quick Configuration** To quickly configure the GGSN parameters, copy the following statements and paste them into the router terminal window:

```
[edit unified-edge gateways ggsn-pgw PGW]
set home-plmn mcc 421 mnc 342
edit gtp
set gn interface lo0.0 v4-address 99.1.1.1
```

**Step-by-Step Procedure** To define a broadband gateway GTP configuration, from the customer edge to the provider network:

1. Define the broadband gateway as P-GW.  

```
user@host# edit unified-edge gateways ggsn-pgw PGW
```
2. Define the home public land mobile network (HPLMN), mobile country code (MCC), and mobile network code (MNC).  

```
[edit unified-edge gateways ggsn-pgw PGW]
user@host# set home-plmn mcc 421 mnc 342
```
3. Configure the GTP settings.  

```
user@host# edit unified-edge gateways ggsn-pgw PGW gtp
```

4. Configure the Gn interface for receiving GTP-C and GTP-U packets on the GGSN to use the loopback interface and IP address specified.

```
[edit unified-edge gateways ggsn-pgw PGW gtp ]
user@host# set gn interface lo0.0 v4-address 99.1.1.1
```

**Results** Check the results of the configuration:

```
user@host# edit unified-edge
user@host# show
unified-edge {
  gateways {
    ggsn-pgw PGW {
      gtp {
        path-management disable;
        gn {
          interface lo0.0 v4-address 99.1.1.1;
        }
        traceoptions {
          file gtp_local size 1m;
          level all;
          flag all;
        }
      }
      home-plmn mcc 421 mnc 342;
    }
  }
}
```

## Verification

To confirm that the configuration is working properly, perform the following tasks:

- [Verifying the Mobile Address Pool on page 657](#)
- [Verifying the Gateway Configuration on page 658](#)

### Verifying the Mobile Address Pool

**Purpose** Verify the mobile pool address assignments.

**Action**

```
user@host# show access address-assignment mobile-pools default-ipv4-address-pool
family inet {
  network {
    29.0.0.0/8 {
      range {
        r1 {
          low 29.0.0.1;
          high 29.255.255.254;
        }
      }
    }
  }
}
default-pool;
```

**Meaning** The output shows the subnet and available address ranges for the mobile pool.

## Verifying the Gateway Configuration

---

**Purpose** Verify the configuration of the GGSN/P-GW gateways.

**Action**

```
user@host# show unified-edge gateways
ggsn-pgw PGW {
  gtp {
    path-management disable;
    gn {
      interface lo0.0 v4-address 200.6.88.1;
    }
    s5 {
      interface lo0.0 v4-address 200.6.88.1;
    }
  }
  home-plmn {
    mcc 421 mnc 342;
  }
}
```

- Related Documentation**
- [Configuring GTP Services Overview on page 302](#)
  - [Configuring a Local Policy on page 537](#)
  - [Configuring GTP Trace Options on page 323](#)
  - [Configuring GTP Services on the Gn Interface on page 312](#)
  - [Configuring a Loopback Interface for Transport of GTP Packets on page 304](#)

## Example: Configuring MobileNext Broadband Gateway

---

This example describes how to configure the MobileNext Broadband Gateway without any provider edge functionality.

- [Requirements on page 658](#)
- [Overview on page 658](#)
- [Configuration on page 660](#)
- [Verification on page 677](#)

### Requirements

This example uses the following hardware and software components:

- Junos OS Release 11.2W
- Juniper Networks MobileNext Broadband Gateway

### Overview

This example describes how to configure the broadband gateway without any provider edge functionality. VPN routing and forwarding (VRF) is used to support the following configuration:



- 3GPP interfaces (Gn and S5) are in the same VRF.
- 3GPP interfaces (Gp and S8) are in the same VRF.
- Gi interfaces (Gi, SGi) to the external networks are in their own VRF named VRF-wireless1.juniper.net and VRF-wireless2.juniper.net, respectively.
- RADIUS server is in its own VRF called RADIUS.
- Charging (Ga) is in its own VRF called CGF.
- DHCPv4 and DHCPv6 proxy clients are in their own VRF called DHCP.

**Table 61: Components of the Broadband Gateway**

Property	Settings	Description
Loopback address	lo0 11.11.11.1/32	Identifies the device for communications.
	lo0 11.11.11.2/32	
	lo0 11.11.11.3/32	
	lo0 11.11.11.11/32	
	lo0 11.11.11.12/32	
	lo0 11.11.11.13/32	
Routing protocol	isis	Indicates the device is using IS-IS and BGP as routing protocols.
	bgp group	
MPLS protocol and LSP definition	mpls label-switched-path pe1-to-pe2 to 10.255.28.17	Indicates the device is using the MPLS protocol with the specified LSP to reach the other core device (pe2).
RSVP	rsvp lo0.0	Indicates the device is using RSVP. The statement must specify the loopback address and the core interfaces that will be used for the RSVP session.
Interface family	family inet	The logical units of the core interfaces belong to family inet, family iso, and family mpls.
	family iso	
	family mpls	
Core interfaces	ge-5/2/0.0 with IP address 33.33.0.1/16	
	ge-5/2/1.0 with IP address 33.44.0.1/16	
	ge-5/3/0.0 with IP address 33.55.0.1/16	
	ge-5/3/1.0 with IP address 33.66.0.1/16	
Gi interface	ge-0/0/0 with IP address 44.44.0.1/16	
Gn interface	ge-5/1/0 with IP address 22.5.0.1/16	

Table 61: Components of the Broadband Gateway (*continued*)

Property	Settings	Description
CGF VRF	ge-0/0/6.0 with IP address 2.2.2.1/16 lo0.2, lo0.12	
RADIUS VRF	ge-0/0/7.0 with IP address 3.3.3.1/16 lo0.11	
DHCP VRF	ge-0/0/8.0 with IP address 4.4.4.1/16 lo0.13	
VRF-wireless1.juniper.net	mif.1	
VRF-wireless2.juniper.net	ge-0/0/0.0 mif.2	

## Configuration

- [Configuring the Chassis on page 660](#)
- [Configuring the IPv4 Interfaces on page 662](#)
- [Enabling IS-IS on page 662](#)
- [Enabling MPLS and RSVP Routing on page 663](#)
- [Configuring BGP on page 664](#)
- [Enabling the Routing Instance for the Layer 3 VPN on page 665](#)
- [Configuring RADIUS Servers on page 665](#)
- [Configuring DHCP Proxy Clients on page 666](#)
- [Enabling the APN Configuration on page 667](#)
- [Configuring Offline Charging on page 670](#)
- [Configuring GTP Services on page 673](#)
- [Configuring AAA on page 675](#)
- [Configuring APN Parameters on page 675](#)

### Configuring the Chassis

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set chassis redundancy graceful-switchover
set system commit synchronize
load merge /etc/config/mobility-defaults.conf
set chassis fpc 1 pic 0 apply-groups mobility
set chassis fpc 1 pic 1 apply-groups mobility
```

```

set chassis fpc 3 pic 0 apply-groups mobility
set chassis fpc 3 pic 1 apply-groups mobility
set chassis fpc 0 forwarding-packages mobility ggsn-pgw
set chassis fpc 5 forwarding-packages mobility ggsn-pgw
set interfaces lo0 unit 1 family inet address 11.11.11.1/32
set interfaces lo0 unit 2 family inet address 11.11.11.2/32
set interfaces lo0 unit 3 family inet address 11.11.11.3/32
set interfaces lo0 unit 11 family inet address 11.11.11.11/32
set interfaces lo0 unit 12 family inet address 11.11.11.12/32
set interfaces lo0 unit 13 family inet address 11.11.11.13/32

```

### Step-by-Step Procedure

To configure the chassis:

1. Enable graceful restart for Routing Engine redundancy.  

```

[edit]
user@pe1# set chassis redundancy graceful-switchover

```
2. Load and merge the default configuration file for the **mobility** group.  

```

[edit]
user@pe1# load merge /etc/config/mobility-defaults.conf

```
3. Configure the **mobility** group on the session DPCs.  

```

[edit]
user@pe1# set chassis fpc 1 pic 0 apply-groups mobility
user@pe1# set chassis fpc 1 pic 1 apply-groups mobility
user@pe1# set chassis fpc 3 pic 0 apply-groups mobility
user@pe1# set chassis fpc 3 pic 1 apply-groups mobility

```



**NOTE:** You must include every services PIC configured with the `jservices-mobile` package at the `[edit unified-edge gateways ggsn-pgw gateway-name system anchor-spics]` hierarchy level on the broadband gateway. If you do not include the services PIC as an anchor interface, then the services PIC will not be used by the broadband gateway.

4. Configure the interface DPC or MPC at the FPC level.  

```

[edit]
user@pe1# set chassis fpc 0 forwarding-packages mobility ggsn-pgw
user@pe1# set chassis fpc 5 forwarding-packages mobility ggsn-pgw

```



**NOTE:** You must include every Packet Forwarding Engine configured with the `ggsn-pgw` forwarding package at the `[edit unified-edge gateways ggsn-pgw gateway-name system anchor-pfes]` hierarchy level on the broadband gateway. If you do not specify the Packet Forwarding Engine as an anchor interface, then the Packet Forwarding Engine will not be used by the broadband gateway.

5. Configure loopback interfaces.

```
[edit]
user@pe1# set interfaces lo0 unit 1 family inet address 11.11.11.1/32
user@pe1# set interfaces lo0 unit 2 family inet address 11.11.11.2/32
user@pe1# set interfaces lo0 unit 3 family inet address 11.11.11.3/32
user@pe1# set interfaces lo0 unit 11 family inet address 11.11.11.11/32
user@pe1# set interfaces lo0 unit 12 family inet address 11.11.11.12/32
user@pe1# set interfaces lo0 unit 13 family inet address 11.11.11.13/32
```

---

### Configuring the IPv4 Interfaces

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set interfaces ge-0/0/0 unit 0 family inet address 44.44.0.1/16
set interfaces ge-0/0/6 unit 0 family inet address 2.2.2.1/16
set interfaces ge-0/0/7 unit 0 family inet address 3.3.3.1/16
set interfaces ge-0/0/8 unit 0 family inet address 4.4.4.1/16
set interfaces ge-5/1/0 unit 0 family inet address 22.5.0.1/16
set interfaces ge-5/2/0 unit 0 family inet address 33.33.0.1/16
set interfaces ge-5/2/1 unit 0 family inet address 33.44.0.1/16
set interfaces ge-5/3/0 unit 0 family inet address 33.55.0.1/16
set interfaces ge-5/3/1 unit 0 family inet address 33.66.0.1/16
```

**Step-by-Step Procedure** To configure the IPv4 interfaces:

1. Configure IPv4 interfaces for the Gi interface.

```
[edit]
user@pe1# set interfaces ge-0/0/0 unit 0 family inet address 44.44.0.1/16
```

2. Configure IPv4 interfaces for the Gn interfaces.

```
[edit]
user@pe1# set interfaces ge-5/1/0 unit 0 family inet address 22.5.0.1/16
```

3. Configure IPv4 interfaces for core routing.

```
[edit]
user@pe1# set interfaces ge-5/2/0 unit 0 family inet address 33.33.0.1/16
user@pe1# set interfaces ge-5/2/1 unit 0 family inet address 33.44.0.1/16
user@pe1# set interfaces ge-5/3/0 unit 0 family inet address 33.55.0.1/16
user@pe1# set interfaces ge-5/3/1 unit 0 family inet address 33.66.0.1/16
```

4. Configure IPv4 interfaces for the charging, RADIUS, and DHCP VRFs.

```
[edit]
user@pe1# set interfaces ge-0/0/6 unit 0 family inet address 2.2.2.1/16
user@pe1# set interfaces ge-0/0/7 unit 0 family inet address 3.3.3.1/16
user@pe1# set interfaces ge-0/0/8 unit 0 family inet address 4.4.4.1/16
```

---

### Enabling IS-IS

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
```

```

set interfaces ge-5/2/0 unit 0 family iso
set interfaces ge-5/2/1 unit 0 family iso
set interfaces ge-5/3/0 unit 0 family iso
set interfaces ge-5/3/1 unit 0 family iso
top
set protocols isis interface ge-5/2/0.0
set protocols isis interface ge-5/2/1.0
set protocols isis interface ge-5/3/0.0
set protocols isis interface ge-5/3/1.0
set protocols isis interface lo0.0

```

### Step-by-Step Procedure

To enable IS-IS routing:

1. Configure the ISO family on interfaces running IS-IS.

```

[edit]
user@pe1# set interfaces ge-5/2/0 unit 0 family iso
user@pe1# set interfaces ge-5/2/1 unit 0 family iso
user@pe1# set interfaces ge-5/3/0 unit 0 family iso
user@pe1# set interfaces ge-5/3/1 unit 0 family iso

```

2. Create the IS-IS interface.

```

[edit]
user@pe1# set protocols isis interface ge-5/2/0.0
user@pe1# set protocols isis interface ge-5/2/1.0
user@pe1# set protocols isis interface ge-5/3/0.0
user@pe1# set protocols isis interface ge-5/3/1.0

```

3. Configure a network entity title on the loopback interface.

```

[edit]
user@pe1# set protocols isis interface lo0.0

```

### Enabling MPLS and RSVP Routing

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```

[edit]
set interfaces ge-5/2/0 unit 0 family mpls
set interfaces ge-5/2/1 unit 0 family mpls
set interfaces ge-5/3/0 unit 0 family mpls
set interfaces ge-5/3/1 unit 0 family mpls
set protocols rsvp interface ge-5/2/0.0
set protocols rsvp interface ge-5/2/1.0
set protocols rsvp interface ge-5/3/0.0
set protocols rsvp interface ge-5/3/1.0
set protocols rsvp interface lo0.0
set protocols mpls explicit-null
set protocols mpls label-switched-path PE-1-to-PE-2 to 10.255.28.17
set protocols mpls interface ge-5/3/1.0
set protocols mpls interface ge-5/3/0.0
set protocols mpls interface ge-5/2/0.0
set protocols mpls interface ge-5/2/1.0

```

**Step-by-Step  
Procedure**

To enable MPLS and RSVP:

1. Configure the interfaces with MPLS enabled.

```
[edit]
user@pe1# set interfaces ge-5/2/0 unit 0 family mpls
user@pe1# set interfaces ge-5/2/1 unit 0 family mpls
user@pe1# set interfaces ge-5/3/0 unit 0 family mpls
user@pe1# set interfaces ge-5/3/1 unit 0 family mpls
```

2. Include the interfaces in the MPLS and RSVP protocol configuration.

```
[edit]
user@pe1# set protocols rsvp interface ge-5/2/0.0
user@pe1# set protocols rsvp interface ge-5/2/1.0
user@pe1# set protocols rsvp interface ge-5/3/0.0
user@pe1# set protocols rsvp interface ge-5/3/1.0
user@pe1# set protocols rsvp interface lo0.0
user@pe1# set protocols mpls interface ge-5/2/0.0
user@pe1# set protocols mpls interface ge-5/2/1.0
user@pe1# set protocols mpls interface ge-5/3/0.0
user@pe1# set protocols mpls interface ge-5/3/1.0
```

3. In the MPLS configuration, advertise label 0 and specify the LSP used for dynamic MPLS.

```
[edit]
user@pe1# set protocols mpls explicit-null
user@pe1# set protocols mpls label-switched-path PE-1-to-PE-2 to 10.255.28.17
```

### Configuring BGP

---

**CLI Quick  
Configuration**

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set routing-options nonstop-routing
set routing-options router-id 10.102.32.59
set routing-options autonomous-system 69
set routing-options forwarding-table export pplb
set protocols bgp group L3VPN-Sig type internal
set protocols bgp group L3VPN-Sig local-address 10.102.32.59
set protocols bgp group L3VPN-Sig family inet-vpn any
set protocols bgp group L3VPN-Sig neighbor 10.255.28.17
```

**Step-by-Step  
Procedure**

To configure BGP:

1. Configure the routing options.

```
[edit]
user@pe1# set routing-options nonstop-routing
user@pe1# set routing-options router-id 10.102.32.59
user@pe1# set routing-options autonomous-system 69
user@pe1# set routing-options forwarding-table export pplb
```

2. Configure the BGP group for Layer 3 VPNs.

```
[edit]
```

```

user@pe1# set protocols bgp group L3VPN-Sig type internal
user@pe1# set protocols bgp group L3VPN-Sig local-address 10.102.32.59
user@pe1# set protocols bgp group L3VPN-Sig family inet-vpn any
user@pe1# set protocols bgp group L3VPN-Sig neighbor 10.255.28.17

```

### Enabling the Routing Instance for the Layer 3 VPN

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```

[edit]
set routing-instances VRF-wireless1.juniper.net instance-type vrf
set routing-instances VRF-wireless1.juniper.net route-distinguisher 10.102.32.59:512
set routing-instances VRF-wireless1.juniper.net vrf-target target:5000:1012
set routing-instances VRF-wireless1.juniper.net vrf-table-label

```

**Step-by-Step Procedure** To configure the routing instance for the VRF used in the Layer 3 VPN:

1. Specify VRF as the type.

```

[edit]
user@pe1# set routing-instances VRF-wireless1.juniper.net instance-type vrf

```

2. Configure the Layer 3 VPN routing instance.

```

[edit]
user@pe1# set routing-instances VRF-wireless1.juniper.net route-distinguisher
10.102.32.59:512
user@pe1# set routing-instances VRF-wireless1.juniper.net vrf-target
target:5000:1012
user@pe1# set routing-instances VRF-wireless1.juniper.net vrf-table-label

```

### Configuring RADIUS Servers

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```

[edit]
set access radius servers radius_server address 3.3.3.2
set access radius servers radius_server secret "$9$TF6ABlcvWxp0WxNdG4QFn"
set access radius servers radius_server accounting-secret
"$9$TQ6Apu1hyKO1b2aU.mOIReclKM8"
set access radius servers radius_server source-interface lo0.11
set access radius servers radius_server source-interface ipv4-address 11.11.11.11
set access radius network-elements radius_ne server radius_server
set routing-instances RADIUS instance-type virtual-router
set routing-instances RADIUS interface ge-0/0/7.0
set routing-instances RADIUS interface lo0.11

```

**Step-by-Step Procedure** To configure the RADIUS servers to interact with the broadband gateway:

1. Configure the RADIUS server.

```

[edit]
user@pe1# set access radius servers radius_server address 3.3.3.2

```

```
user@pe1# set access radius servers radius_server secret
"$9$TF6ABlcVWxp0WxNdG4QFn"
user@pe1# set access radius servers radius_server accounting-secret
"$9$TQ6Apu1hyKO1b2aU.mO1REclKM8"
user@pe1# set access radius servers radius_server source-interface lo0.11
ipv4-address 11.11.11.11
```

2. Specify the RADIUS server as a network element.

```
[edit]
user@pe1# set access radius network-elements radius_ne server radius_server
```

3. Specify the routing instance for the RADIUS accounting server.

```
[edit]
user@pe1# set routing-instances RADIUS instance-type virtual-router
user@pe1# set routing-instances RADIUS interface ge-0/0/7.0
user@pe1# set routing-instances RADIUS interface lo0.11
```

---

### Configuring DHCP Proxy Clients

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set routing-instances DHCP instance-type virtual-router
set routing-instances DHCP system services dhcp-proxy-client dhcpv4-profiles dhcp-1
  bind-interface ge-0/0/8.0
set routing-instances DHCP system services dhcp-proxy-client dhcpv4-profiles dhcp-1
  servers 4.4.4.2 priority 1
set routing-instances DHCP system services dhcp-proxy-client dhcpv4-profiles dhcp-1
  servers 4.4.4.3 priority 2
set routing-instances DHCP interface ge-0/0/8.0
set routing-instances DHCP interface lo0.13
```

#### Step-by-Step Procedure

To configure DHCP proxies:

1. Configure the DHCP proxy clients by associating them with the host interface and prioritized DHCP servers.

```
[edit]
user@pe1# set routing-instances DHCP system services dhcp-proxy-client
  dhcpv4-profiles dhcp-1 bind-interface ge-0/0/8.0
user@pe1# set routing-instances DHCP system services dhcp-proxy-client
  dhcpv4-profiles dhcp-1 servers 4.4.4.2 priority 1
user@pe1# set routing-instances DHCP system services dhcp-proxy-client
  dhcpv4-profiles dhcp-1 servers 4.4.4.3 priority 2
```

2. Specify the routing instance for the DHCP server.

```
[edit]
user@pe1# set routing-instances DHCP instance-type virtual-router
user@pe1# set routing-instances DHCP interface ge-0/0/8.0
user@pe1# set routing-instances DHCP interface lo0.13
```



### Enabling the APN Configuration

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set interfaces mif unit 1 family inet
set interfaces mif unit 2 family inet
set interfaces ms-1/1/0 unit 16000 family inet
set interfaces ms-3/1/0 unit 16000 family inet
set routing-instances VRF-wireless1.juniper.net instance-type vrf
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
  wireless-juniper1 family inet network 100.100.0.0/16 range r1 low 100.100.0.0
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
  wireless-juniper1 family inet network 100.100.0.0/16 range r1 high 100.100.255.255
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
  wireless-juniper1 family inet network 200.200.0.0/16
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
  wireless-juniper1 family inet network 100.102.0.0/16 range r2 low 100.102.0.0
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
  wireless-juniper1 family inet network 100.102.0.0/16 range r2 high 100.102.255.255
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
  wireless-juniper1 family inet network 100.103.0.0/16 range r3 low 100.103.0.0
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
  wireless-juniper1 family inet network 100.103.0.0/16 range r3 high 100.103.255.255
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
  wireless-juniper1 family inet network 100.104.0.0/16 range r4 low 100.104.0.0
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
  wireless-juniper1 family inet network 100.104.0.0/16 range r4 high 100.104.255.255
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
  wireless-juniper1 family inet network 100.105.0.0/16 range r5 low 100.105.0.0
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
  wireless-juniper1 family inet network 100.105.0.0/16 range r5 high 100.105.255.255
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
  wireless-juniper1 family inet network 100.106.0.0/16 range r6 low 100.106.0.0
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
  wireless-juniper1 family inet network 100.106.0.0/16 range r6 high 100.106.255.255
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
  wireless-juniper1 family inet network 100.107.0.0/16 range r7 low 100.107.0.0
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
  wireless-juniper1 family inet network 100.107.0.0/16 range r7 high 100.107.255.255
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
  wireless-juniper1 family inet network 100.108.0.0/16 range r8 low 100.108.0.0
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
  wireless-juniper1 family inet network 100.108.0.0/16 range r8 high 100.108.255.255
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
  wireless-juniper1 family inet network 100.109.0.0/16 range r9 low 100.109.0.0
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
  wireless-juniper1 family inet network 100.109.0.0/16 range r9 high 100.109.255.255
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
  wireless-juniper1 family inet network 100.110.0.0/16 range r10 low 100.110.0.0
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
  wireless-juniper1 family inet network 100.110.0.0/16 range r10 high 100.110.255.255
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
  wireless-juniper1 family inet network 100.111.0.0/16 range r11 low 100.111.0.0
```

```

set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
wireless-juniper1 family inet network 100.111.0.0/16 range r11 high 100.111.255.255
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
wireless-juniper1 family inet network 100.112.0.0/16 range r12 low 100.112.0.0
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
wireless-juniper1 family inet network 100.112.0.0/16 range r12 high 100.112.255.255
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
wireless-juniper1 family inet network 100.113.0.0/16 range r13 low 100.113.0.0
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
wireless-juniper1 family inet network 100.113.0.0/16 range r13 high 100.113.255.255
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
wireless-juniper1 family inet network 100.114.0.0/16 range r14 low 100.114.0.0
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
wireless-juniper1 family inet network 100.114.0.0/16 range r14 high 100.114.255.255
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
wireless-juniper1 family inet network 100.115.0.0/16 range r15 low 100.115.0.0
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
wireless-juniper1 family inet network 100.115.0.0/16 range r15 high 100.115.255.255
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
wireless-juniper1 family inet network 100.116.0.0/16 range r16 low 100.116.0.0
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
wireless-juniper1 family inet network 100.116.0.0/16 range r16 high 100.116.255.255
set routing-instances VRF-wireless2.juniper.net instance-type virtual-router
set routing-instances VRF-wireless2.juniper.net access address-assignment mobile-pools
wireless-juniper1 family inet network 100.100.0.0/16 range r1 low 100.100.0.0
set routing-instances VRF-wireless2.juniper.net access address-assignment mobile-pools
wireless-juniper1 family inet network 100.100.0.0/16 range r1 high 100.100.255.255
set routing-instances VRF-wireless2.juniper.net access address-assignment mobile-pools
wireless-juniper1 family inet network 200.200.0.0/16
set routing-instances VRF-wireless2.juniper.net interface ge-0/0/0.0
set routing-instances VRF-wireless2.juniper.net interface mif.2

```

### Step-by-Step Procedure

To enable the APN configuration:

1. Create mobile interfaces.  

```

[edit]
user@pe1# set interfaces mif unit 1 family inet
user@pe1# set interfaces mif unit 2 family inet
user@pe1# set interfaces ms-1/1/0 unit 16000 family inet
user@pe1# set interfaces ms-3/1/0 unit 16000 family inet

```
2. Configure the VRF-wireless1.juniper.net routing instance.  

```

[edit]
user@pe1# edit routing-instances VRF-wireless1.juniper.net

```
3. Specify the IP pool configuration for the VRF-wireless1.juniper.net routing instance.  

```

[edit routing-instances VRF-wireless1.juniper.net]
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.100.0.0/16 range r1 low 100.100.0.0
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.100.0.0/16 range r1 high 100.100.255.255
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 200.200.0.0/16

```

---

Copyright © 2013, Juniper Networks, Inc. 669

```

user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.116.0.0/16 range r2 low 100.116.0.0
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.116.0.0/16 range r2 high 100.116.255.255

```

4. Configure the IP pool configuration for the VRF-wireless2.juniper.net routing instance.

```

[edit routing-instances VRF-wireless2.juniper.net]
user@pe1# set routing-instances VRF-wireless2.juniper.net access
address-assignment mobile-pools wireless-juniper1 family inet network
100.100.0.0/16 range r1 low 100.100.0.0
user@pe1# set routing-instances VRF-wireless2.juniper.net access
address-assignment mobile-pools wireless-juniper1 family inet network
100.100.0.0/16 range r1 high 100.100.255.255
user@pe1# set routing-instances VRF-wireless2.juniper.net access
address-assignment mobile-pools wireless-juniper1 family inet network
200.200.0.0/16
user@pe1# set routing-instances VRF-wireless2.juniper.net interface ge-0/0/0.0
user@pe1# set routing-instances VRF-wireless2.juniper.net interface mif.2

```

### Configuring Offline Charging

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```

[edit]
set routing-instances CHR-VRF instance-type vrf
set routing-instances CHR-VRF interface lo0.12
set routing-instances CHR-VRF route-distinguisher 10.102.32.59:1000
set routing-instances CHR-VRF vrf-target target:5000:1000
set routing-instances CHR-VRF vrf-table-label
set routing-instances CHR-VRF-Local instance-type virtual-router
set routing-instances CHR-VRF-Local interface ge-0/0/6.0
set routing-instances CHR-VRF-Local interface lo0.2
set unified-edge gateways ggsn-pgw MBG1 charging cdr-profiles cdr-wireless1.juniper.net
enable-reduced-partial-cdrs
set unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles CGW-trig-pro-1 offline
volume-limit 1048576
set unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles CGW-trig-pro-1 offline
volume-limit direction both
set unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles
trigr-wireless1.juniper.net offline volume-limit 1048576
set unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles
trigr-wireless1.juniper.net offline volume-limit direction uplink
set unified-edge gateways ggsn-pgw MBG1 charging transport-profiles CGW-trans-pro-1
offline charging-gateways cdr-release r7
set unified-edge gateways ggsn-pgw MBG1 charging transport-profiles CGW-trans-pro-1
offline charging-gateways peer-order peer my_cgfw
set unified-edge gateways ggsn-pgw MBG1 charging transport-profiles CGW-trans-pro-1
offline charging-gateways peer-order peer local_cgfw
set unified-edge gateways ggsn-pgw MBG1 charging transport-profiles CGW-trans-pro-1
offline charging-gateways switch-back-time 1
set unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
trans-wireless1.juniper.net offline charging-gateways cdr-release r7

```

```

set unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
  trans-wireless1.juniper.net offline charging-gateways persistent-storage-order
  local-storage
set unified-edge gateways ggsn-pgw MBG1 charging local-persistent-storage-options
  file-age 60
set unified-edge gateways ggsn-pgw MBG1 charging local-persistent-storage-options
  file-format raw-asn
set unified-edge gateways ggsn-pgw MBG1 charging local-persistent-storage-options
  disk-space-policy water-mark-level1 percentage 70
set unified-edge gateways ggsn-pgw MBG1 charging local-persistent-storage-options
  disk-space-policy water-mark-level2 percentage 80
set unified-edge gateways ggsn-pgw MBG1 charging local-persistent-storage-options
  disk-space-policy water-mark-level3 percentage 90
set unified-edge gateways ggsn-pgw MBG1 charging charging-profiles CGW-chr-pro-1
  profile-id 2
set unified-edge gateways ggsn-pgw MBG1 charging charging-profiles CGW-chr-pro-1
  transport-profile CGW-trans-pro-1
set unified-edge gateways ggsn-pgw MBG1 charging charging-profiles CGW-chr-pro-1
  trigger-profile CGW-trig-pro-1
set unified-edge gateways ggsn-pgw MBG1 charging charging-profiles
  chr-wireless1.juniper.net profile-id 1
set unified-edge gateways ggsn-pgw MBG1 charging charging-profiles
  chr-wireless1.juniper.net transport-profile trans-wireless1.juniper.net
set unified-edge gateways ggsn-pgw MBG1 charging charging-profiles
  chr-wireless1.juniper.net cdr-profile cdr-wireless1.juniper.net
set unified-edge gateways ggsn-pgw MBG1 charging charging-profiles
  chr-wireless1.juniper.net trigger-profile trigr-wireless1.juniper.net
set unified-edge gateways ggsn-pgw MBG1 charging gtp transport-protocol tcp
set unified-edge gateways ggsn-pgw MBG1 charging gtp version v0
set unified-edge gateways ggsn-pgw MBG1 charging gtp header-type long
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer local_cgwr
  destination-ipv4-address 42.42.0.2
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer local_cgwr source-interface
  lo0.2
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer local_cgwr source-interface
  ipv4-address 11.11.11.2
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer local_cgwr destination-port
  3386
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer local_cgwr transport-protocol
  tcp
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer local_cgwr n3-requests 1
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer local_cgwr t3-response 3
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer local_cgwr header-type long
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer local_cgwr
  pending-queue-size 1000
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer my_cgfr
  destination-ipv4-address 41.41.0.2
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer my_cgfr source-interface
  lo0.12
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer my_cgfr source-interface
  ipv4-address 11.11.11.12
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer my_cgfr destination-port
  3386
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer my_cgfr transport-protocol
  tcp
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer my_cgfr n3-requests 1

```

```
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer my_cgf t3-response 5
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer my_cgf header-type long
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer my_cgf pending-queue-size
1000
```

**Step-by-Step  
Procedure**

To configure the offline charging profile:

1. Create the routing instances for charging. CHR-VRF is for the external charging gateway and CHR-VRF-Local is for persistent local storage.  
  
[edit]  
user@pe1# set routing-instances CHR-VRF instance-type vrf  
user@pe1# set routing-instances CHR-VRF interface lo0.12  
user@pe1# set routing-instances CHR-VRF route-distinguisher 10.102.32.59:1000  
user@pe1# set routing-instances CHR-VRF vrf-target target:5000:1000  
user@pe1# set routing-instances CHR-VRF vrf-table-label  
user@pe1# set routing-instances CHR-VRF-Local instance-type virtual-router  
user@pe1# set routing-instances CHR-VRF-Local interface ge-0/0/6.0  
user@pe1# set routing-instances CHR-VRF-Local interface lo0.2
2. Configure charging for the GGSN called MBG1.  
  
[edit]  
user@pe1# edit unified-edge gateways ggsn-pgw MBG1 charging
3. Specify the global GTP Prime properties to transmit CDRs to the external charging gateway.  
  
[edit unified-edge gateways ggsn-pgw MBG1 charging]  
user@pe1# set gtp transport-protocol tcp  
user@pe1# set gtp version v0  
user@pe1# set gtp header-type long
4. Specify the GTP Prime properties for the GTP Prime peers.  
  
[edit unified-edge gateways ggsn-pgw MBG1 charging]  
user@pe1# set gtp peer local\_cgwr destination-ipv4-address 42.42.0.2  
user@pe1# set gtp peer local\_cgwr source-interface lo0.2  
user@pe1# set gtp peer local\_cgwr source-interface ipv4-address 11.11.11.2  
user@pe1# set gtp peer local\_cgwr destination-port 3386  
user@pe1# set gtp peer local\_cgwr transport-protocol tcp  
user@pe1# set gtp peer local\_cgwr n3-requests 1  
user@pe1# set gtp peer local\_cgwr t3-response 3  
user@pe1# set gtp peer local\_cgwr header-type long  
user@pe1# set gtp peer local\_cgwr pending-queue-size 1000  
user@pe1# set gtp peer my\_cgwr destination-ipv4-address 41.41.0.2  
user@pe1# set gtp peer my\_cgwr source-interface lo0.12  
user@pe1# set gtp peer my\_cgwr source-interface ipv4-address 11.11.11.12  
user@pe1# set gtp peer my\_cgwr destination-port 3386  
user@pe1# set gtp peer my\_cgwr transport-protocol tcp  
user@pe1# set gtp peer my\_cgwr n3-requests 1  
user@pe1# set gtp peer my\_cgwr t3-response 5  
user@pe1# set gtp peer my\_cgwr header-type long  
user@pe1# set gtp peer my\_cgwr pending-queue-size 1000
5. Configure local persistent storage of the CDRs.  
  
[edit unified-edge gateways ggsn-pgw MBG1 charging]  
user@pe1# set local-persistent-storage-options file-age 60

```

user@pe1# set local-persistent-storage-options file-format raw-asn
user@pe1# set local-persistent-storage-options disk-space-policy water-mark-level1
percentage 70
user@pe1# set local-persistent-storage-options disk-space-policy water-mark-level2
percentage 80
user@pe1# set local-persistent-storage-options disk-space-policy water-mark-level3
percentage 90

```

6. Configure the transport, trigger, and CDR profiles referenced by the charging profile for offline charging.

```

[edit unified-edge gateways ggsn-pgw MBG1 charging]
user@pe1# set transport-profiles CGW-trans-pro-1 offline charging-gateways
cdr-release r7
user@pe1# set transport-profiles CGW-trans-pro-1 offline charging-gateways
peer-order peer my_cgf
user@pe1# set transport-profiles CGW-trans-pro-1 offline charging-gateways
peer-order peer local_cgw
user@pe1# set transport-profiles CGW-trans-pro-1 offline charging-gateways
switch-back-time 1
user@pe1# set transport-profiles trans-wireless1.juniper.net offline
charging-gateways cdr-release r7
user@pe1# set transport-profiles trans-wireless1.juniper.net offline
charging-gateways persistent-storage-order local-storage
user@pe1# set trigger-profiles CGW-trig-pro-1 offline volume-limit 1048576
user@pe1# set trigger-profiles CGW-trig-pro-1 offline volume-limit direction both
user@pe1# set trigger-profiles trigr-wireless1.juniper.net offline volume-limit 1048576
user@pe1# set trigger-profiles trigr-wireless1.juniper.net offline volume-limit direction
uplink
user@pe1# set cdr-profiles cdr-wireless1.juniper.net enable-reduced-partial-cdrs

```

7. Configure the charging profile. The CGW-chr-pro-1 charging profile is used for the external charging gateway, while the chr-wireless1.juniper.net charging profile is used for local persistent storage.

```

[edit unified-edge gateways ggsn-pgw MBG1 charging]
user@pe1# set charging-profiles CGW-chr-pro-1 profile-id 2
user@pe1# set charging-profiles CGW-chr-pro-1 transport-profile CGW-trans-pro-1
user@pe1# set charging-profiles CGW-chr-pro-1 trigger-profile CGW-trig-pro-1
user@pe1# set charging-profiles chr-wireless1.juniper.net profile-id 1
user@pe1# set charging-profiles chr-wireless1.juniper.net transport-profile
trans-wireless1.juniper.net
user@pe1# set charging-profiles chr-wireless1.juniper.net cdr-profile
cdr-wireless1.juniper.net
user@pe1# set charging-profiles chr-wireless1.juniper.net trigger-profiles
trigr-wireless1.juniper.net
user@pe1# set charging-profiles chr-wireless1.juniper.net trigger-profile
trigr-wireless1.juniper.net

```

### Configuring GTP Services

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```

[edit]
set unified-edge gateways ggsn-pgw MBG1 gtp gn interface lo0.1

```

```
set unified-edge gateways ggsn-pgw MBG1 gtp gn interface v4-address 11.11.11.1
set unified-edge gateways ggsn-pgw MBG1 gtp gn n3-requests 3
set unified-edge gateways ggsn-pgw MBG1 gtp gn t3-response 3
set unified-edge gateways ggsn-pgw MBG1 gtp gn echo-interval 60
set unified-edge gateways ggsn-pgw MBG1 gtp gn path-management enable
set unified-edge gateways ggsn-pgw MBG1 gtp gp interface lo0.1
set unified-edge gateways ggsn-pgw MBG1 gtp gp interface v4-address 11.11.11.1
set unified-edge gateways ggsn-pgw MBG1 gtp gp n3-requests 3
set unified-edge gateways ggsn-pgw MBG1 gtp gp t3-response 3
set unified-edge gateways ggsn-pgw MBG1 gtp gp echo-interval 60
set unified-edge gateways ggsn-pgw MBG1 gtp gp path-management enable
set unified-edge gateways ggsn-pgw MBG1 gtp s5 interface lo0.1
set unified-edge gateways ggsn-pgw MBG1 gtp s5 interface v4-address 11.11.11.1
set unified-edge gateways ggsn-pgw MBG1 gtp s5 n3-requests 3
set unified-edge gateways ggsn-pgw MBG1 gtp s5 t3-response 3
set unified-edge gateways ggsn-pgw MBG1 gtp s5 echo-interval 60
set unified-edge gateways ggsn-pgw MBG1 gtp s5 path-management enable
set unified-edge gateways ggsn-pgw MBG1 gtp s8 interface lo0.1
set unified-edge gateways ggsn-pgw MBG1 gtp s8 interface v4-address 11.11.11.1
set unified-edge gateways ggsn-pgw MBG1 gtp s8 n3-requests 3
set unified-edge gateways ggsn-pgw MBG1 gtp s8 t3-response 3
set unified-edge gateways ggsn-pgw MBG1 gtp s8 echo-interval 60
set unified-edge gateways ggsn-pgw MBG1 gtp s8 path-management enable
```

#### Step-by-Step Procedure

To configure GTP services:

1. Configure the GTP services for the GGSN called MBG1.

```
[edit]
```

```
user@pe1# edit unified-edge gateways ggsn-pgw MBG1 gtp
```

2. Configure GTP services for the Gn, Gp, S5, and S8 interfaces with path management enabled. The same address must be specified for all addresses.

```
[edit unified-edge gateways ggsn-pgw MBG1 gtp]
```

```
user@pe1# set gn interface lo0.1
```

```
user@pe1# set gn interface v4-address 11.11.11.1
```

```
user@pe1# set gn n3-requests 3
```

```
user@pe1# set gn t3-response 3
```

```
user@pe1# set gn echo-interval 60
```

```
user@pe1# set gn path-management enable
```

```
user@pe1# set gp interface lo0.1
```

```
user@pe1# set gp interface v4-address 11.11.11.1
```

```
user@pe1# set gp n3-requests 3
```

```
user@pe1# set gp t3-response 3
```

```
user@pe1# set gp echo-interval 60
```

```
user@pe1# set gp path-management enable
```

```
user@pe1# set s5 interface lo0.1
```

```
user@pe1# set s5 interface v4-address 11.11.11.1
```

```
user@pe1# set s5 n3-requests 3
```

```
user@pe1# set s5 t3-response 3
```

```
user@pe1# set s5 echo-interval 60
```

```
user@pe1# set s5 path-management enable
```

```
user@pe1# set s8 interface lo0.1
```

```
user@pe1# set s8 interface v4-address 11.11.11.1
```

```
user@pe1# set s8 n3-requests 3
```

```
user@pe1# set s8 t3-response 3
```



```
user@pe1# set s8 echo-interval 60
user@pe1# set s8 path-management enable
```

### Configuring AAA

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge aaa mobile-profiles aaa_profile radius authentication network-element
radius_ne
set unified-edge aaa mobile-profiles aaa_profile radius accounting network-element
radius_ne
set unified-edge aaa mobile-profiles aaa_profile radius options nas-ip-address 11.11.11.1
set unified-edge aaa mobile-profiles aaa_profile radius attributes exclude calling-station-id
access-request
set unified-edge aaa mobile-profiles aaa_profile radius attributes exclude event-time-stamp
accounting-start
```

**Step-by-Step Procedure** To configure AAA profiles:

1. Configure the AAA profile called `aaa_profile` for the broadband gateway.
 

```
[edit]
user@pe1# edit unified-edge aaa mobile-profiles aaa_profile
```
2. Specify the RADIUS authentication and accounting settings for the profile.
 

```
[edit unified-edge aaa mobile-profiles aaa_profile]
user@pe1# set radius authentication network-element radius_ne
user@pe1# set radius accounting network-element radius_ne
```
3. Specify the RADIUS options.
 

```
[edit unified-edge aaa mobile-profiles aaa_profile]
user@pe1# set radius options nas-ip-address 11.11.11.1
```
4. Specify the RADIUS attributes to exclude from the message type.
 

```
[edit unified-edge aaa mobile-profiles aaa_profile]
user@pe1# set radius attributes exclude calling-station-id access-request
user@pe1# set radius attributes exclude event-time-stamp accounting-start
```

### Configuring APN Parameters

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless1.juniper.net apn-type
real
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless1.juniper.net
apn-data-type ipv4
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless1.juniper.net
mobile-interface mif.1
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless1.juniper.net
address-assignment local
```

```
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless1.juniper.net
  address-assignment inet-pool pool wireless-juniper1
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless1.juniper.net
  session-timeout 2
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless1.juniper.net
  idle-timeout 60
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless1.juniper.net charging
  default-charging-profile chr-wireless1.juniper.net
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless1.juniper.net
  selection-mode from-ms
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless2.juniper.net apn-type
  real
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless2.juniper.net
  apn-data-type ipv4
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless2.juniper.net
  mobile-interface mif.2
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless2.juniper.net
  address-assignment local
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless2.juniper.net
  address-assignment inet-pool pool wireless-juniper1
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless2.juniper.net
  address-assignment dhcpv4-proxy-client-profile logical-system default routing-instance
  DHCP profile-name dhcp-1
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless2.juniper.net
  session-timeout 2
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless2.juniper.net
  idle-timeout 60
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless2.juniper.net
  aaa-profile aaa_profile
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless2.juniper.net charging
  default-charging-profile CGW-chr-pro-1
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless2.juniper.net
  selection-mode from-ms
```

#### Step-by-Step Procedure

To configure APN services:

1. Configure the APN services for the GGSN called MBG1.  
  
[edit]  
user@pe1# edit unified-edge gateways ggsn-pgw MBG1 apn-services
2. Configure the wireless1.juniper.net APN used for the mif.1 interface. This APN uses the wireless-juniper1 IP pool for address assignment and chr-wireless1.juniper.net as the default charging profile.  
  
[edit unified-edge gateways ggsn-pgw MBG1 apn-services]  
user@pe1# set apn wireless1.juniper.net apn-type real  
user@pe1# set apn wireless1.juniper.net apn-data-type ipv4  
user@pe1# set apn wireless1.juniper.net mobile-interface mif.1  
user@pe1# set apn wireless1.juniper.net address-assignment local  
user@pe1# set apn wireless1.juniper.net address-assignment inet-pool pool wireless-juniper1  
user@pe1# set apn wireless1.juniper.net session-timeout 2  
user@pe1# set apn wireless1.juniper.net idle-timeout 60  
user@pe1# set apn wireless1.juniper.net charging default-charging-profile chr-wireless1.juniper.net

```
user@pe1# set apn wireless1.juniper.net selection-mode from-ms
```

3. Configure the wireless2.juniper.net APN used for the mif.2 interface. This APN uses the wireless-juniper1 IP pool or dhcpv4-proxy-client-profile for address assignment. This APN uses aaa\_profile as the AAA profile and CGW-chr-pro-1 as the default charging profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services]
user@pe1# set apn wireless2.juniper.net apn-type real
user@pe1# set apn wireless2.juniper.net apn-data-type ipv4
user@pe1# set apn wireless2.juniper.net mobile-interface mif.2
user@pe1# set apn wireless2.juniper.net address-assignment local
user@pe1# set apn wireless2.juniper.net address-assignment inet-pool pool
wireless-juniper1
user@pe1# set apn wireless2.juniper.net address-assignment
dhcpv4-proxy-client-profile logical-system default routing-instance DHCP
profile-name
user@pe1# set apn wireless2.juniper.net session-timeout 2
user@pe1# set apn wireless2.juniper.net idle-timeout 60
user@pe1# set apn wireless2.juniper.net aaa-profile aaa_profile
user@pe1# set apn wireless2.juniper.net charging default-charging-profile
CGW-chr-pro-1
user@pe1# set apn wireless2.juniper.net selection-mode from-ms
```

## Verification

### Verifying MPLS LSP Status

**Purpose** Verify the MPLS LSP status for GGSN initiation.

**Action**

```
user@pe1> show mpls lsp
```

Ingress LSP: 1 sessions

To	From	State	Rt	P	ActivePath	LSPname
10.255.28.17	10.102.32.59	Up	0	*		PE-1-to-PE-2

Total 1 displayed, Up 1, Down 0

Egress LSP: 1 sessions

To	From	State	Rt	Style	Labelin	Labelout	LSPname
10.102.32.59	10.255.28.17	Up	0	1 FF	0		- PE-2-to-PE-1

Total 1 displayed, Up 1, Down 0

Transit LSP: 0 sessions

Total 0 displayed, Up 0, Down 0

**Meaning** The `show mpls lsp` command displays information about the configured label-switched paths, including the destination address.

### Verifying Layer 3 VPN Status

**Purpose** Verify Layer 3 VPN status and routes for GGSN initiation and successful call establishment.

**Action** user@pe1> show route table VRF-wireless1.juniper.net  
VRF-wireless1.juniper.net.inet.0: 14 destinations, 14 routes (14 active, 0  
holddown, 0 hidden)  
+ = Active Route, - = Last Active, \* = Both

```
11.11.11.1/32      *[Direct/0] 01:08:14
                  > via lo0.10
55.55.0.0/16       *[BGP/170] 00:15:55, localpref 100, from 10.255.28.17
                  AS path: I
                  > to 33.55.0.2 via ge-5/3/0.0, label-switched-path PE-1-to-PE-2
100.104.172.0/22   *[Anchor/7] 00:04:53
                  Private indexed

100.104.176.0/22   *[Anchor/7] 00:04:52
                  Private indexed
100.104.180.0/22   *[Anchor/7] 00:04:51
                  Private indexed
100.105.20.0/22    *[Anchor/7] 00:04:53
                  Private indexed
100.105.24.0/22    *[Anchor/7] 00:04:52
                  Private indexed
100.105.28.0/22    *[Anchor/7] 00:04:51
                  Private indexed
100.105.32.0/22    *[Anchor/7] 00:04:50
                  Private indexed
100.105.36.0/22    *[Anchor/7] 00:04:50
                  Private indexed
run show unified-edge ggsn-pgw resource-manager clients | no-more
100.105.40.0/22    *[Anchor/7] 00:04:49
                  Private indexed
100.105.136.0/22   *[Anchor/7] 00:04:50
                  Private indexed
100.105.140.0/22   *[Anchor/7] 00:04:50
                  Private indexed
100.105.144.0/22   *[Anchor/7] 00:04:49
                  Private indexed
```

**Meaning** The **show route table** command verifies the Layer 3 VPN configuration by displaying the VRF table for the specified VRF.

---

### Verifying Session DPCs and Interface DPCs Initialization

---

**Purpose** Verify the initialization of session DPCs and interface DPCs for GGSN initiation.

```

Action user@pe1> show chassis fpc pic-status
Slot 0 Online MPC Type 2 3D EQ
PIC 0 Online 10x 1GE(LAN) SFP
PIC 1 Online 10x 1GE(LAN) SFP
PIC 2 Online 10x 1GE(LAN) SFP
PIC 3 Online 10x 1GE(LAN) SFP
Slot 1 Online MS-DPC EM
PIC 0 Online MS-DPC PIC
PIC 1 Online MS-DPC PIC
Slot 2 Online MPC Type 2 3D EQ
PIC 0 Online 10x 1GE(LAN) SFP
PIC 1 Online 10x 1GE(LAN) SFP
PIC 2 Online 10x 1GE(LAN) SFP
PIC 3 Online 10x 1GE(LAN) SFP
Slot 3 Online MS-DPC EM
PIC 0 Online MS-DPC PIC
PIC 1 Online MS-DPC PIC
Slot 4 Online MPC Type 2 3D EQ
PIC 0 Online 2x 10GE XFP
PIC 1 Online 2x 10GE XFP
PIC 2 Online 10x 1GE(LAN) SFP
PIC 3 Online 10x 1GE(LAN) SFP
Slot 5 Online MPC Type 2 3D EQ
PIC 0 Online 10x 1GE(LAN) SFP
PIC 1 Online 10x 1GE(LAN) SFP
PIC 2 Online 10x 1GE(LAN) SFP
PIC 3 Online 10x 1GE(LAN) SFP

user@pe1> show unified-edge ggsn-pgw resource-manager clients
Client State Role Type
apfe-0/1 In-Service RMS_PRIMARY RCM-PFE
apfe-0/0 In-Service RMS_PRIMARY RCM-PFE
ms-1/0 In-Service RMS_PRIMARY RCM-SP
ms-1/1 In-Service RMS_PRIMARY RCM-SP
apfe-2/1 In-Service RMS_SECONDARY RCM-PFE
apfe-2/0 In-Service RMS_SECONDARY RCM-PFE
ms-3/0 In-Service RMS_SECONDARY RCM-SP
ms-3/1 In-Service RMS_SECONDARY RCM-SP
apfe-4/1 In-Service RMS_PRIMARY RCM-PFE
apfe-4/0 In-Service RMS_PRIMARY RCM-PFE
apfe-5/1 In-Service RMS_SECONDARY RCM-PFE
apfe-5/0 In-Service RMS_SECONDARY RCM-PFE

```

**Meaning** The `show chassis fpc pic-status` command lists the PIC status. It shows that the DPCs are initialized if the status is Online.

The `show unified-edge ggsn-pgw resource-manager clients` command lists the state for resource manager clients. It displays the In-Service state to indicate that the DPCs are initialized.

### Verifying Broadband Gateway Status

**Purpose** Verify the status and statistics on the broadband gateway for GGSN initiation, call establishment, and Gn-to-Gi connectivity across the MPLS core.

```
Action  user@pe1> show unified-edge ggsn-pgw status
        Mobile gateway status:
        Active Subscribers   :           180
        Active Sessions      :           180
        Active Bearers       :           180
        CPU Load (%)         :             0
        Memory Load (%)      :            27

user@pe1> show unified-edge ggsn-pgw statistics
Control plane statistics:
  Session establishment attempts:        200180
  Successful session establishments:      200180
  MS/peer initiated session deactivations: 199611
  Successful MS/peer initiated deactivations: 389
  Gateway initiated session deactivations: 389
  Successful gateway initiated deactivations: 389
Data plane GTP statistics (Gn/S5/S8):
  Input   packets:      88696
  Input   bytes:       7805248
  Output  packets:      87843
  Output  bytes:       7730184
  Discarded packets:    0
Data plane GTP statistics (Gi):
  Input   packets:      87843
  Input   bytes:       7730184
  Output  packets:      88696
  Output  bytes:       7805248
  Discarded packets:    0
```

**Meaning** The **show unified-edge ggsn-pgw status** command displays the status of the broadband gateway, including the number of active subscribers, active sessions, and active bearers. It also displays the CPU load and memory load.

The **show unified-edge ggsn-pgw statistics** command displays the control plane and data plane statistics for the broadband gateway.

---

### Verifying Session Establishment

**Purpose** Verify the session establishment for call establishment and Gn-to-Gi connectivity across the MPLS core.

```

Action user@pe1> show unified-edge ggsn-pgw subscribers
      IMSI                MSISDN          Subscriber
                        Address          Peer
                        Address          Address          APN
333444444444535        34444535    100.105.24.1    22.0.111.111
wireless1.juniper.net
6664444444449456        64494456    100.105.36.3    88.2.111.111
wireless1.juniper.net
999114444444489        91444489    100.105.28.14   99.0.111.111
wireless1.juniper.net
888455444444518        84554518    100.105.28.5    55.0.111.111
wireless1.juniper.net
222444444444552        222444552    100.105.24.19   22.2.222.223
wireless1.juniper.net

user@pe1> show unified-edge ggsn-pgw subscribers extensive
Subscriber Information:
  IMSI: 333444444444535    IMEI: 1122334455667874
  MSISDN: 34444535        Time Zone: None    (DST): None
  Status: Home
User Location Info:
  MCC: None MNC: None
  LAC: 0x0 CI: 0x0    SAC: 0x0 RAC: 0x0 TAC: 0x0 ECI: 0x0
  RAT Type: Unknown
PDN Session:
  APN name: wireless1.juniper.net
  IPv4 Address: 100.105.24.1    IPv6 Address: None
  Direct Tunnel: Disabled    Session Duration: 4:52
  Local Control address: 11.11.11.1 Remote Control address: 22.0.111.111
  TEID Control Local: 0xa01944a TEID Control Remote: 0x1b28a
  Addressing scheme: Local    Selection mode: sub verified
  Session PIC: 1 /0 (FPC/PIC) Anchor PFE: 0 /0 (FPC/PIC)
  Session State: Established    GTP Version: 1
  Serving network: MCC: None MNC :None
Bearer:
  NSAPI/EBI: 5    Charging ID: 0xa01944a
  Local Data address: 11.11.11.1 Remote Data address: 22.0.111.111
  Local TEID: 0x420400 Remote TEID: 0x1b289
  Bearer State: Established Substate: -
  Idle Timeout: 60 min(188-0,0) AAA Interim Interval: 0 min(0 -0,0)
Negotiated QoS Parameters:
  Traffic Class:Background    ARP: 1
  Traffic Handling Priority:3    Transfer Delay :10
  MBR Uplink: 8640 kbps    MBR Downlink :8640 kbps
  Signaling Indicator :0
  Forwarding Class: -    Loss Priority: -
Requested QoS Parameters:
  Traffic Class: Background    ARP: 1
  Traffic Handling Priority: 3    Transfer Delay: 10
  MBR Uplink : 8640 kbps    MBR Downlink: 8640 kbps
  Signaling Indicator: 0
Charging information:
  Profile ID: 1 Profile name: chr-wireless1.juniper.net
  State: Ready Previous State: Ga
  Profile selection criteria: Static default
  Details: Accounting enabled, Offline bearer
Offline charging information:
  Current service data container sequence number: 0
  Current partial record sequence number : 0
  Number of CDRs closed : 0
Rating group information:
  Rating group: 0 Service id: 0

```

```
Action ID: 0x101944a          Trigger profile: 2
Change condition bitmask: 0x0 Action-id-bitmask: 0x1
Signal bitmask: 0x0           Last signal bitmask: 0x0
Details: Bearer trigger, Offline RG
Last statistics collection time : None collected
```

```
.
.
.
```

**Meaning** The `show unified-edge ggsn-pgw subscribers` command lists the established sessions.

The `show unified-edge ggsn-pgw subscribers extensive` command displays detailed information about these subscribers.

### Verifying GTP-C Status

---

**Purpose** Verify the GTP-C status for call establishment.



```

Action user@pe1> show unified-edge ggsn-pgw gtp peer
Rmt IP Address          Local IP Address          Routing-Instance
-----
88.5.100.100            11.11.11.1              10
88.0.100.100            11.11.11.1              8
88.0.100.104            11.11.11.1              8
88.0.111.111           11.11.11.1              8

user@pe1> show unified-edge ggsn-pgw gtp peer remote-address 88.0.111.111 detail
Peer Detail:
-----
Remote IP Addr          = 88.0.111.111
Local IP Addr           = 11.11.11.1
Routing Instance        = 8
Interface Type          = GTP_INTF_GN
GTP Version             = 1
RCM Registration Done   = yes
Is Restart Counter Valid = yes
Restart Counter Value   = 1
Sent Restart Counter Value = 7
Control Path N3 Req     = 3
Control Path T3 Timer   = 5
Control Path Echo N3 Req = 8
Control Path Echo T3 Timer = 15
Control Path Echo Interval = 60
Is PATH Management Enabled (control) = no
Is CSID Supported       = no
IS GTP-C using Short Seq Number = no
GTP-C Path State        = inactive
Data Path N3 Req        = 8
Data Path T3 Timer      = 15
Data Path Echo Interval = 60
Is PATH Management Enabled (Data) = no
GTP-U Path State        = inactive

user@pe1> show unified-edge ggsn-pgw gtp statistics
Global Packet Statistics
Received Packets Dropped : 0
Packet Allocation Fail   : 0
Packet Send Fail         : 0
IP Version Error Received : 0
IP Protocol Error Received : 0
GTP Port Error Received  : 0
Packet Length Error Received : 0
Unknown Messages Received : 0

GTP Version 0 Statistics:
-----
Protocol Error           : 0
Unsupported Messages Received : 0
T3 Response Timer Expires : 0

Message Type              Received      Transmitted
-----
Total number of messages  63           63
Total number of bytes     4158         4032
Redirect messages         0            0
Echo Request              0            0
Echo Response             0            0
Version Not Supported     0            0

```

Create PDP Context Request	63	0
Create PDP Context Response	0	63
Update PDP Context Request	0	0
Update PDP Context Response	0	0
Delete PDP Context Request	0	0
Delete PDP Context Response	0	0

## GTP Version 1 Statistics:

```
-----
Protocol Error                : 0
Unsupported Messages Received : 0
T3 Response Timer Expires    : 0
```

Message Type	Received	Transmitted
-----	-----	-----
Total number of messages	216464	217110
Total number of bytes	13611840	9676412
Redirect messages	0	0
Echo Request	0	0
Echo Response	0	0
Version Not Supported	0	620
Create PDP Context Request	116474	0
Create PDP Context Response	0	116474
Update PDP Context Request	0	0
Update PDP Context Response	0	0
Delete PDP Context Request	99990	23
Delete PDP Context Response	0	99990

## GTP Version 2 Statistics:

```
-----
Protocol Error                : 0
Unsupported Messages Received : 0
T3 Response Timer Expires    : 0
```

Message Type	Received	Transmitted
-----	-----	-----
Total number of messages	219727	219473
Total number of bytes	24348253	12581846
Redirect messages	0	0
Echo Request	0	0
Echo Response	0	0
Version Not Supported	0	0
Create session request	120080	0
Create session response	0	119460
Modify bearer request	0	0
Modify bearer response	0	0
Delete session request	99647	0
Delete session response	0	99647
Create bearer request	0	0
Create bearer response	0	0
Update bearer request	0	0
Update bearer response	0	0
Delete bearer request	0	366
Delete bearer response	0	0
Delete PDN connection set request	0	0
Delete PDN connection set response	0	0
Update PDN connection set request	0	0
Update PDN connection set response	0	0
Modify bearer command	0	0

Modify bearer failure indication	0	0
Delete bearer command	0	0
Delete bearer failure indication	0	0
Bearer resource command	0	0
Bearer resource failure indication	0	0
Change notification request	0	0
Change notification response	0	0

## Error Indication Statistics:

Version	Received	Transmitted
-----	-----	-----
GTPv0	0	0
GTPv1	0	3

**Meaning** The `show unified-edge ggsn-pgw gtp peer` command displays the GTP peers.

The `show unified-edge ggsn-pgw gtp peer remote-address address detail` command displays detailed information about the specified GTP peer.

The `show unified-edge ggsn-pgw gtp statistics` command displays the GTP statistics.

### Verifying Charging Status

**Purpose** Verify the charging status for call establishment.

```

Action user@pe1> show unified-edge ggsn-pgw charging transfer status
Charging Transfer Status
Transport-Profile : CGW-TRANS-pro-1
  Total UnAck CDR's      : 19995
  Total Buffered CDR's   : 280005

Transport-Profile : trans-wireless1.juniper.net
  Total UnAck CDR's      : 0
  Total Buffered CDR's   : 50000

user@pe1> show unified-edge ggsn-pgw charging transfer statistics
Charging Transfer Statistics
Transport-Profile : CGW-TRANS-pro-1
  Redirection Requests    Rx: 0      Redirection Responses    Tx: 0
  DRT Responses           Rx: 0      DRT Requests             Tx: 4000
  DRT successful Responses Rx: 0      DRT Error Responses       Rx: 0
  DRT Requests timed out  : 334525 CGF Switch Back Times    : 64
  Batch Requests          Tx: 0      Batch Response Errors     Rx: 0
  Batch CDR's            Tx: 0      CDR Count                 : 19995
  Total WFA               : 4000

Transport-Profile : trans-wireless1.juniper.net
  Redirection Requests    Rx: 0      Redirection Responses    Tx: 0
  DRT Responses           Rx: 0      DRT Requests             Tx: 0
  DRT successful Responses Rx: 0      DRT Error Responses       Rx: 0
  DRT Requests timed out  : 0        CGF Switch Back Times    : 0
  Batch Requests          Tx: 1362   Batch Response Errors     Rx: 0
  Batch CDR's            Tx: 50000   CDR Count                 : 50000
  Total WFA               : 0

user@pe1> show unified-edge ggsn-pgw charging local-persistent-storage statistics
Charging local-persistent-storage Statistics
  Batch Messages received      : 1362
  Batch Responses sent         : 1362
  Invalid Messages received    : 0
  Number of temp log files opened : 1
  Number of journal files opened : 1
  Number of journal files closed : 0
  Number of CDR log files closed : 0
  Number of CDR files closed due to file-age : 0
  Number of CDR files closed due to file-size : 0
  Number of CDR files closed due to cdr-count : 0
  Abnormal file closures      : 0
  Normal file closures        : 0
  Number of CDR log files closed in TS_32_297 format : 0
  Number of CDR log files closed in raw asn1 format : 0
  Total number of CDRs backed up : 50000
  Disk Full messages sent      : 0
  Disk Full resolve messages sent : 0
  Number of async IO reqs written : 1362
  Number of CDR storage files on disk : 3
  Disk space status            : DISK_AVAILABLE
  Current storage space in use(MB) : 6685
  Available storage space on disk(MB) : 27862
  Total storage space on disk(MB) : 34547
  Watermark level1 at(MB)      : 24182(70%)
  Watermark level2 at(MB)      : 27637(80%)
  Watermark level3 at(MB)      : 31092(90%)

Temporary CDR log file Statistics
File Name: /var/db/mobility/charging/ggsn/temp_log/templog_file_1.log

```

```
Journal file name       : /var/db/mobility/charging/ggsn/jrn1/jrn1_1.log
Current number of CDRs  : 50000
Current file size(bytes) : 10357039
File age trigger(mins)  : 60
File size trigger(bytes) : 10485760
CDR count trigger       : 0
```

**Meaning** The **show unified-edge ggsn-pgw charging transfer status** command displays the charging transfer status. It also displays information about the CDR transfers for the transport profiles.

The **show unified-edge ggsn-pgw charging transfer statistics** command displays the charging transfer statistics for the transport profiles.

The **show unified-edge ggsn-pgw charging local-persistent-storage statistics** command displays the charging statistics for local persistent storage.

---

### Verifying Mobile Interfaces

**Purpose** Verify there is no data loss across the mobile interfaces for call establishment and Gn-to-Gi connectivity across the MPLS core.

**Action**    user@pe1> show interfaces mif.1 extensive

```
Logical interface mif.1 (Index 85) (SNMP ifIndex 812) (Generation 165)
Flags: SNMP-Traps Encapsulation: GTP-over-MIF
Bandwidth: 1000mbps
Traffic statistics:
  Input bytes   :          6160000
  Output bytes  :          6084936
  Input packets :           70000
  Output packets:           69147
Local statistics:
  Input bytes   :              0
  Output bytes  :              0
  Input packets :              0
  Output packets:              0
Transit statistics:
  Input bytes   :          6160000          0 bps
  Output bytes  :          6084936          0 bps
  Input packets :           70000          0 pps
  Output packets:           69147          0 pps
Protocol inet, MTU: 1440, Generation: 219, Route table: 12
Flags: Sendbroadcast-pkt-to-re, Is-Primary
```

```
user@pe1> show interfaces mif.2 extensive
Logical interface mif.2 (Index 86) (SNMP ifIndex 813) (Generation 166)
Flags: SNMP-Traps Encapsulation: GTP-over-MIF
Bandwidth: 1000mbps
Traffic statistics:
  Input bytes   :              0
  Output bytes  :              0
  Input packets :              0
  Output packets:              0
Local statistics:
  Input bytes   :              0
  Output bytes  :              0
  Input packets :              0
  Output packets:              0
Transit statistics:
  Input bytes   :              0          0 bps
  Output bytes  :              0          0 bps
  Input packets :              0          0 pps
  Output packets:              0          0 pps
Protocol inet, MTU: 1440, Generation: 220, Route table: 13
Flags: Sendbroadcast-pkt-to-re
```

**Meaning**    The `show interfaces mif.number extensive` command displays detailed information about the specified mobile interface.

**Related Documentation**

- [Example: Configuring MobileNext Broadband Gateway with Provider Edge Functionality on page 689](#)
- [Example: Simple Unified Edge Configuration on page 651](#)

## Example: Configuring MobileNext Broadband Gateway with Provider Edge Functionality

This example describes how to configure the MobileNext Broadband Gateway integrated with provider edge functionality.

- [Requirements on page 689](#)
- [Overview on page 689](#)
- [Configuration on page 690](#)
- [Verification on page 696](#)

### Requirements

This example uses the following hardware and software components:

- Junos OS Release 11.2W
- Juniper Networks MobileNext Broadband Gateway

Before you configure the broadband gateway, make sure you have the following information:

- IP addresses for configuring GPRS tunneling protocol (GTP), RADIUS, and charging signaling functions.
- MPLS provider-edge configuration details for MX 3D Universal Edge Routers, including BGP peer configuration, IP addresses, AS number, import/export route target, and IGP configuration.

### Overview

This example describes how to configure the broadband gateway integrated with provider edge functionality. VPN routing and forwarding (VRF) is used to support the following configuration:

- Internal BGP is used to exchange VPN routing information between the provider edge routers.
- RSVP is used in the MPLS backbone to establish the label-switched paths (LSPs) between the provider edge routers.



**NOTE:** All routing instances are VRF routing instances in the MPLS VPN.

- 3GPP interfaces (Gn and S5) for control are in the same VRF called VRF11-Control.
- 3GPP interfaces (Gn and S5) for data are in the same VRF called VRF11-Data.
- 3GPP interfaces (Gp and S8) for control are in the same VRF called VRF12-Control.
- 3GPP interfaces (Gp and S8) for data are in the same VRF called VRF12-Data.

- Gi interfaces (Gi, SGi) to the external networks are in the same VRF named VRF3.
- RADIUS server and charging are in the VRF called VRF2.

**Table 62: Components of the Broadband Gateway**

Property	Settings	Description
Loopback address	lo0 unit 100 address 192.168.100.1/32 lo0 unit 111 address 192.168.111.1/32 lo0 unit 112 address 192.168.112.1/32 lo0 unit 121 address 192.168.121.1/32 lo0 unit 122 address 192.168.122.1/32 lo0 unit 200 address 192.168.200.1/32	Interfaces used for 3GPP signaling and IP routing functions
Routing protocol	bgp	Indicates device is using BGP as routing protocol
MPLS protocol and LSP definition	mpls	Indicates device is using the MPLS protocol
RSVP	rsvp	Indicates device is using RSVP
Gi/SGi routing instance	VRF3 mif.0	Mobile interface unit 0 (mif unit 0) is associated with Gi/SGi routing instance by placing the interface in VRF3
Gn/S5 control connectivity	VRF11-Control lo0.111	VRF for Gn/S5 interfaces for control
Gn/S5 data connectivity	VRF11-Data lo0.112	VRF for Gn/S5 interfaces for data
Gp/S8 control connectivity	VRF12-Control lo0.121	VRF for Gp/S8 interfaces for control
Gp/S8 data connectivity	VRF12-Data lo0.122	VRF for Gp/S8 interfaces for data
RADIUS/charging connectivity	VRF2 lo0.200	VRF for charging and RADIUS servers

## Configuration

- [Configuring the Chassis on page 691](#)
- [Configuring the MPLS/BGP VPN on page 692](#)
- [Enabling the Routing Instances for the VPN on page 693](#)



- [Configuring GTP Interfaces on page 694](#)
- [Configuring the Source Interface for RADIUS and Charging Servers on page 695](#)
- [Enabling the APN Configuration on page 695](#)

### Configuring the Chassis

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
load merge /etc/config/mobility-defaults.conf
set chassis fpc 1 pic 0 apply-groups mobility
set chassis fpc 1 pic 1 apply-groups mobility
set chassis fpc 3 pic 0 apply-groups mobility
set chassis fpc 3 pic 1 apply-groups mobility
set chassis fpc 0 forwarding-packages mobility ggsn-pgw
set chassis fpc 5 forwarding-packages mobility ggsn-pgw
set interfaces lo0 unit 100 family inet address 192.168.100.1/32
set interfaces lo0 unit 111 family inet address 192.168.111.1/32
set interfaces lo0 unit 112 family inet address 192.168.112.1/32
set interfaces lo0 unit 121 family inet address 192.168.121.1/32
set interfaces lo0 unit 122 family inet address 192.168.122.1/32
set interfaces lo0 unit 200 family inet address 192.168.200.1/32
set chassis fpc 5 pic 2 tunnel-services bandwidth 10g
set interfaces vt-5/2/0 unit 0 family inet
```

#### Step-by-Step Procedure

To configure the chassis:

1. Load and merge the default configuration file for the **mobility** group.

```
[edit]
user@pe1# load merge /etc/config/mobility-defaults.conf
```

2. Configure the **mobility** group on the session DPCs.

```
[edit]
user@pe1# set chassis fpc 1 pic 0 apply-groups mobility
user@pe1# set chassis fpc 1 pic 1 apply-groups mobility
user@pe1# set chassis fpc 3 pic 0 apply-groups mobility
user@pe1# set chassis fpc 3 pic 1 apply-groups mobility
```



**NOTE:** You must include every services PIC configured with the **jservices-mobile** package at the **[edit unified-edge gateways ggsn-pgw gateway-name system anchor-spics]** hierarchy level on the broadband gateway. If you do not include the services PIC as an anchor interface, then the services PIC will not be used by the broadband gateway.

3. Configure the interface MPC at the FPC level.

```
[edit]
user@pe1# set chassis fpc 0 forwarding-packages mobility ggsn-pgw
user@pe1# set chassis fpc 5 forwarding-packages mobility ggsn-pgw
```



**NOTE:** You must include every Packet Forwarding Engine configured with the `ggsn-pgw` forwarding package at the `[edit unified-edge gateways ggsn-pgw gateway-name system anchor-pfes]` hierarchy level on the broadband gateway. If you do not specify the Packet Forwarding Engine as an anchor interface, then the Packet Forwarding Engine will not be used by the broadband gateway.

4. Configure loopback interfaces for signaling functions.

```
[edit]
user@pe1# set interfaces lo0 unit 100 family inet address 192.168.100.1/32
user@pe1# set interfaces lo0 unit 111 family inet address 192.168.111.1/32
user@pe1# set interfaces lo0 unit 112 family inet address 192.168.112.1/32
user@pe1# set interfaces lo0 unit 121 family inet address 192.168.121.1/32
user@pe1# set interfaces lo0 unit 122 family inet address 192.168.122.1/32
user@pe1# set interfaces lo0 unit 200 family inet address 192.168.200.1/32
```

5. Configure the tunnel interfaces.

```
[edit]
user@pe1# set chassis fpc 5 pic 2 tunnel-services bandwidth 10g
user@pe1# set interfaces vt-5/2/0 unit 0 family inet
```

### Configuring the MPLS/BGP VPN

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set protocols mpls label-switched-path LSP1 to 192.168.100.5
set protocols mpls label-switched-path LSP1 no-cspf
set protocols mpls interface xe-1/0/1
set protocols rsvp interface xe-1/0/1
set protocols bgp local-as 14203
set protocols bgp group PE1-PE2 type internal
set protocols bgp group PE1-PE2 local-address 192.168.100.1
set protocols bgp group PE1-PE2 family inet-vpn unicast
set protocols bgp group PE1-PE2 neighbor 192.168.100.5
```

#### Step-by-Step Procedure

To enable MPLS and RSVP:

1. In the MPLS configuration, specify the LSP used for dynamic MPLS and disable constrained-path LSP computation.

```
[edit]
user@pe1# set protocols mpls label-switched-path LSP1 to 192.168.100.5
user@pe1# set protocols mpls label-switched-path LSP1 no-cspf
```

2. Include the interface in the MPLS and RSVP protocol configuration.

```
[edit]
user@pe1# set protocols rsvp interface xe-1/0/1
user@pe1# set protocols mpls interface xe-1/0/1
```

3. Configure the local AS for BGP updates.

```
[edit]
user@pe1# set protocols bgp local-as 14203
```

4. Configure the BGP group for Layer 3 VPNs.

```
[edit]
user@pe1# set protocols bgp group PE1-PE2 type internal
user@pe1# set protocols bgp group PE1-PE2 local-address 192.168.100.1
user@pe1# set protocols bgp group PE1-PE2 family inet-vpn unicast
user@pe1# set protocols bgp group PE1-PE2 neighbor 192.168.100.5
```

### Enabling the Routing Instances for the VPN

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set routing-instances VRF11-Control instance-type vrf
set routing-instances VRF11-Control interface lo0.111
set routing-instances VRF11-Control route-distinguisher 192.168.100.1:111
set routing-instances VRF11-Control vrf-target target:1:111
set routing-instances VRF11-Control vrf-table-label
set routing-instances VRF11-Data instance-type vrf
set routing-instances VRF11-Data interface lo0.112
set routing-instances VRF11-Data route-distinguisher 192.168.100.1:112
set routing-instances VRF11-Data vrf-target target:1:112
set routing-instances VRF11-Data vrf-table-label
set routing-instances VRF12-Control instance-type vrf
set routing-instances VRF12-Control interface lo0.121
set routing-instances VRF12-Control route-distinguisher 192.168.100.1:121
set routing-instances VRF12-Control vrf-target target:1:121
set routing-instances VRF12-Control vrf-table-label
set routing-instances VRF12-Data instance-type vrf
set routing-instances VRF12-Data interface lo0.122
set routing-instances VRF12-Data route-distinguisher 192.168.100.1:122
set routing-instances VRF12-Data vrf-target target:1:122
set routing-instances VRF12-Data vrf-table-label
set routing-instances VRF2 instance-type vrf
set routing-instances VRF2 interface lo0.200
set routing-instances VRF2 route-distinguisher 192.168.100.1:200
set routing-instances VRF2 vrf-target target:1:200
set routing-instances VRF2 interface vt-5/2/0.0
```

#### Step-by-Step Procedure

To configure the routing instance for the VRF used in the Layer 3 VPN:



**BEST PRACTICE:** For GTP traffic, use the vrf-table-label option when configuring the routing instances. For RADIUS or charging traffic, use the tunnel interface when configuring the routing instance.

1. Configure the VRF routing instances for GTP traffic.

```
[edit]
user@pe1# set routing-instances VRF11-Control instance-type vrf
user@pe1# set routing-instances VRF11-Control interface lo0.111
user@pe1# set routing-instances VRF11-Control route-distinguisher 192.168.100.1:111
user@pe1# set routing-instances VRF11-Control vrf-target target:1:111
user@pe1# set routing-instances VRF11-Control vrf-table-label
user@pe1# set routing-instances VRF11-Data instance-type vrf
user@pe1# set routing-instances VRF11-Data interface lo0.112
user@pe1# set routing-instances VRF11-Data route-distinguisher 192.168.100.1:112
user@pe1# set routing-instances VRF11-Data vrf-target target:1:112
user@pe1# set routing-instances VRF11-Data vrf-table-label
user@pe1# set routing-instances VRF12-Control instance-type vrf
user@pe1# set routing-instances VRF12-Control interface lo0.121
user@pe1# set routing-instances VRF12-Control route-distinguisher 192.168.100.1:121
user@pe1# set routing-instances VRF12-Control vrf-target target:1:121
user@pe1# set routing-instances VRF12-Control vrf-table-label
user@pe1# set routing-instances VRF12-Data instance-type vrf
user@pe1# set routing-instances VRF12-Data interface lo0.122
user@pe1# set routing-instances VRF12-Data route-distinguisher 192.168.100.1:122
user@pe1# set routing-instances VRF12-Data vrf-target target:1:122
user@pe1# set routing-instances VRF12-Data vrf-table-label
```

2. Configure the VRF routing instance for RADIUS or charging traffic.

```
[edit]
user@pe1# set routing-instances VRF2 instance-type vrf
user@pe1# set routing-instances VRF2 interface lo0.200
user@pe1# set routing-instances VRF2 route-distinguisher 192.168.100.1:200
user@pe1# set routing-instances VRF2 vrf-target target:1:200
user@pe1# set routing-instances VRF2 interface vt-5/2/0.0
```

### Configuring GTP Interfaces

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge gateways ggsn-pgw MBG1 gtp gn control interface lo0.111
set unified-edge gateways ggsn-pgw MBG1 gtp gn data interface lo0.112
set unified-edge gateways ggsn-pgw MBG1 gtp gp control interface lo0.121
set unified-edge gateways ggsn-pgw MBG1 gtp gp data interface lo0.122
set unified-edge gateways ggsn-pgw MBG1 gtp s5 control interface lo0.111
set unified-edge gateways ggsn-pgw MBG1 gtp s5 data interface lo0.112
set unified-edge gateways ggsn-pgw MBG1 gtp s8 control interface lo0.121
set unified-edge gateways ggsn-pgw MBG1 gtp s8 data interface lo0.122
```

**Step-by-Step Procedure** To configure GTP interfaces:

1. Configure the GTP interfaces for the broadband gateway called MBG1.

```
[edit]
user@pe1# edit unified-edge gateways ggsn-pgw MBG1 gtp
```

2. Specify the appropriate loopback interface associated with the VRF routing instance for the Gn, Gp, S5, and S8 interfaces.

```
[edit unified-edge gateways ggsn-pgw MBG1 gtp]
```

```

user@pe1# set gn control interface lo0.111
user@pe1# set gn data interface lo0.112
user@pe1# set gp control interface lo0.121
user@pe1# set gp data interface lo0.122
user@pe1# set s5 control interface lo0.111
user@pe1# set s5 data interface lo0.112
user@pe1# set s8 control interface lo0.121
user@pe1# set s8 data interface lo0.122

```

### Configuring the Source Interface for RADIUS and Charging Servers

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```

[edit]
set access radius servers radius_server source-interface lo0.200
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer CGF source-interface lo0.200

```

**Step-by-Step Procedure** To associate source interfaces with the RADIUS or charging servers:

1. Specify the source interface for the RADIUS server.

```

[edit]
user@pe1# set access radius servers radius_server source-interface lo0.200

```

2. Specify the source interface for the charging server.

```

[edit]
user@pe1# set unified-edge gateways ggsn-pgw MBG1 charging gtp peer CGF
source-interface lo0.200

```

### Enabling the APN Configuration

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```

[edit]
set interfaces mif unit 0 family inet
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless.juniper.net
apn-data-type ipv4
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless.juniper.net
mobile-interface mif.0
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless.juniper.net
address-assignment local
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless.juniper.net
aaa-profile aaa_profile
set routing-instances VRF3 interface mif unit 0 family inet

```

**Step-by-Step Procedure** To enable the APN configuration:

1. Create the mobile interface for mobile subscribers.

```

[edit]
user@pe1# set interfaces mif unit 0 family inet

```

2. Configure the APN services for mobile subscribers on the broadband gateway called MBG1.

```
[edit]
user@pe1# edit unified-edge gateways ggsn-pgw MBG1 apn-services
```

3. Configure the wireless.juniper.net APN used for the mif.0 interface. This APN uses aaa\_profile as the AAA profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services]
user@pe1# set apns wireless.juniper.net apn-data-type ipv4
user@pe1# set apns wireless.juniper.net mobile-interface mif.0
user@pe1# set apns wireless.juniper.net address-assignment local
user@pe1# set apns wireless.juniper.net aaa-profile aaa_profile
```

4. Specify the VRF routing instance for routing mobile subscriber traffic on the mobile interface.

```
[edit]
user@pe1# set routing-instances VRF3 interface mif unit 0 family inet
```

## Verification

### Verifying MPLS LSP Status

**Purpose** Verify the MPLS LSP status for broadband gateway initiation.

**Action**

```
user@pe1> show mpls lsp
```

Ingress LSP: 1 sessions							
To	From	State	Rt	P	ActivePath	LSPname	
192.168.100.5	10.102.32.59	Up	0	*		LSP1	
Total 1 displayed, Up 1, Down 0							

Egress LSP: 1 sessions							
To	From	State	Rt	Style	Labelin	Labelout	LSPname
10.102.32.59	192.168.100.5	Up	0	1 FF	0	-	LSP2
Total 1 displayed, Up 1, Down 0							

Transit LSP: 0 sessions  
Total 0 displayed, Up 0, Down 0

**Meaning** The **show mpls lsp** command displays information about the configured label-switched paths, including the destination address.

### Verifying Broadband Gateway Status

**Purpose** Verify the status and statistics on the broadband gateway for GGSN/P-GW initiation, call establishment, and Gn-to-Gi connectivity across the MPLS core.

```

Action  user@pe1> show unified-edge ggsn-pgw status
        Mobile gateway status:
        Active Subscribers   :           1
        Active Sessions      :           1
        Active Bearers       :           1
        CPU Load (%)         :           0
        Memory Load (%)      :          28

user@pe1> show unified-edge ggsn-pgw statistics gateway MBG1
Control plane statistics:
  Session establishment attempts:          0
  Successful session establishments:        0
  MS/peer initiated session deactivations: 0
  Successful MS/peer initiated deactivations: 0
  Gateway initiated session deactivations: 0
  Successful gateway initiated deactivations: 0
Data plane GTP statistics (Gn/S5/S8):
  Input   packets:          20
  Input   bytes:          2560
  Output  packets:           0
  Output  bytes:           0
  Discarded packets:        0
Data plane GTP statistics (Gi):
  Input   packets:           0
  Input   bytes:           0
  Output  packets:          20
  Output  bytes:          2560
  Discarded packets:        0

```

**Meaning** The **show unified-edge ggsn-pgw status** command displays the status of the broadband gateway, including the number of active subscribers, active sessions, and active bearers. It also displays the CPU load and memory load.

The **show unified-edge ggsn-pgw statistics** command displays the control plane and data plane statistics for the broadband gateway.

### Verifying Mobile Interfaces

**Purpose** Verify that there is no data loss across the mobile interfaces for call establishment and Gn-to-Gi connectivity across the MPLS core.

```
Action user@pe1> show interfaces mif.0 extensive
Logical interface mif.0 (Index 85) (SNMP ifIndex 812) (Generation 165)
Flags: SNMP-Traps Encapsulation: GTP-over-MIF
Bandwidth: 1000mbps
Traffic statistics:
  Input bytes :          6160000
  Output bytes :         6084936
  Input packets:          70000
  Output packets:         69147
Local statistics:
  Input bytes :           0
  Output bytes :           0
  Input packets:           0
  Output packets:          0
Transit statistics:
  Input bytes :          6160000          0 bps
  Output bytes :         6084936          0 bps
  Input packets:          70000          0 pps
  Output packets:         69147          0 pps
Protocol inet, MTU: 1440, Generation: 219, Route table: 12
Flags: Sendbroadcast-pkt-to-re, Is-Primary
```

**Meaning** The `show interfaces mif.number extensive` command displays detailed information about the specified mobile interface.

- Related Documentation**
- [Example: Configuring MobileNext Broadband Gateway on page 658](#)
  - [Example: Simple Unified Edge Configuration on page 651](#)

---

## Example: Configuring NAT

This example describes how to configure Network Address Translation (NAT) on the MobileNext Broadband Gateway. This simple example illustrates the NAT44 transition scenario. This example only describes the portions of the configuration related to supporting NAT service sets.

- [Requirements on page 698](#)
- [Overview on page 699](#)
- [Configuration on page 699](#)
- [Verification on page 701](#)

### Requirements

This example uses the following hardware and software components:

- Junos OS Release 11.2W
- Juniper Networks MobileNext Broadband Gateway



## Overview

The broadband gateway should be configured as follows to demonstrate this scenario:

- FPC 1 PIC 0 is the session DPC
- FPC 1 PIC 1 is the Multiservices DPC
- Service interface for NAT is ms-1/1/0
- Service set is applied on mif.0
- NAT pool address range is 19.19.19.1 to 19.19.19.32
- NAT rule matches the user equipment (UE) address range 30.30.0.0/16

## Configuration

- [Configuring the Chassis on page 699](#)
- [Configuring NAT Pools and NAT Rules on page 700](#)
- [Configuring Service Sets on page 701](#)

### Configuring the Chassis

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
load merge /etc/config/mobility-defaults.conf
set chassis fpc 1 pic 0 apply-groups mobility
set chassis fpc 1 pic 1 adaptive-services service-package extension-provider control-cores
  1
set chassis fpc 1 pic 1 adaptive-services service-package extension-provider data-cores 7
set chassis fpc 1 pic 1 adaptive-services service-package extension-provider
  object-cache-size 14336
set chassis fpc 1 pic 1 adaptive-services service-package extension-provider policy-db-size
  256
set chassis fpc 1 pic 1 adaptive-services service-package extension-provider package
  jservices-nat
set chassis fpc 1 pic 1 adaptive-services service-package extension-provider package
  jservices-alg
set chassis fpc 1 pic 1 adaptive-services service-package syslog daemon any
set chassis fpc 1 pic 1 adaptive-services service-package syslog kernel any
```

#### Step-by-Step Procedure

To configure the chassis:

1. Load and merge the default configuration file for the **mobility** group.

```
[edit]
user@pe1# load merge /etc/config/mobility-defaults.conf
```

2. Configure the **mobility** group on the session DPC.

```
[edit]
user@pe1# set chassis fpc 1 pic 0 apply-groups mobility
```

3. Configure the Multiservices DPC for NAT services. Specify the `jservices-nat` and `jservices-alg` packages.

```
[edit]
user@pe1# set chassis fpc 1 pic 1 adaptive-services service-package
extension-provider control-cores 1
user@pe1# set chassis fpc 1 pic 1 adaptive-services service-package
extension-provider data-cores 7
user@pe1# set chassis fpc 1 pic 1 adaptive-services service-package
extension-provider object-cache-size 14336
user@pe1# set chassis fpc 1 pic 1 adaptive-services service-package
extension-provider policy-db-size 256
user@pe1# set chassis fpc 1 pic 1 adaptive-services service-package
extension-provider package jservices-nat
user@pe1# set chassis fpc 1 pic 1 adaptive-services service-package
extension-provider package jservices-alg
```

---

### Configuring NAT Pools and NAT Rules

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set services nat pool pool_nat44 address-range low 19.19.19.1 high 19.19.19.32
set services nat pool pool_nat44 port automatic
set services nat rule rule_nat44 match-direction input
set services nat rule rule_nat44 term t1 from source-address 30.30.0.0/16
set services nat rule rule_nat44 term t1 then translated source-pool pool_nat44
set services nat rule rule_nat44 term t1 then translated translation-type napt-44
```

#### Step-by-Step Procedure

To configure NAT pools and NAT rules:

1. Configure the NAT pool address as an address range.

```
[edit]
user@pe1# set services nat pool pool_nat44 address-range low 19.19.19.1 high
19.19.19.32
```

2. Specify that the NAT pool port is a router-assigned port.

```
[edit]
user@pe1# set services nat pool pool_nat44 port automatic
```

3. Configure the NAT rule to match on input.

```
[edit]
user@pe1# set services nat rule rule_nat44 match-direction input
```

4. Specify the input condition for the NAT term.

```
[edit]
user@pe1# set services nat rule rule_nat44 term t1 from source-address 30.30.0.0/16
```

5. Specify the input actions for the NAT term.

```
[edit]
user@pe1# set services nat rule rule_nat44 term t1 then translated source-pool
pool_eif
```

```
user@pe1# set services nat rule rule_nat44 term t1 then translated translation-type
napt-44
```

### Configuring Service Sets

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set interfaces ms-1/1/0 unit 0 family inet
set services service-set set_0 nat-rules rule_nat44
set services service-set set_0 interface-service service-interface ms-1/1/0
set interfaces mif unit 0 family inet service input service-set set_0
set interfaces mif unit 0 family inet service output service-set set_0
```

**Step-by-Step Procedure** To configure service sets:

1. Configure the service interface associated with the service set.

```
[edit]
user@pe1# set interfaces ms-1/1/0 unit 0 family inet
```

2. Configure the service set.

```
[edit]
user@pe1# set services service-set set_0
```

3. Specify the NAT rules.

```
[edit]
user@pe1# set services service-set set_0 nat-rules rule_nat44
```

4. Specify the service interface.

```
[edit]
user@pe1# set services service-set set_0 interface-service service-interface ms-1/1/0
```

5. Associate the service set with the mobile interface.

```
[edit]
user@pe1# set interfaces mif unit 0 family inet service input service-set set_0
user@pe1# set interfaces mif unit 0 family inet service output service-set set_0
```

## Verification

### Verifying the NAT Pool Information

**Purpose** Verify information about NAT pools.

**Action**    `user@pe1> show services nat pool detail`  
Interface: ms-1/1/0, Service set: set\_0  
NAT pool: pool\_nat44, Translation type: napt-44  
Address range: 19.19.19.1-19.19.19.32  
Address range: 2.2.2.2-2.2.2.2  
Port range: 512-65535, Ports in use: 0, Out of port errors: 0, Max ports used: 0

- Related Documentation**
- [Example: Configuring MobileNext Broadband Gateway on page 658](#)
  - [Example: Configuring MobileNext Broadband Gateway with Provider Edge Functionality on page 689](#)

---

## Example: Configuring a Standalone S-GW

This example describes how to configure the MobileNext Broadband Gateway as a standalone Serving Gateway (S-GW). The emphasis is on S-GW configuration, and does not include many other parameters that a full device configuration requires.

- [Requirements on page 702](#)
- [Overview on page 702](#)
- [Configuration on page 702](#)
- [Verification on page 707](#)

### Requirements

This example uses the following hardware and software components:

- Junos OS Release 11.4W
- Juniper Networks MobileNext Broadband Gateway

### Overview

This example describes how to configure the broadband gateway as a standalone S-GW (SGW-MBG1). The S-GW supports the following configuration:

- The S1-U data, S5, and S11 control interface are in the main routing instance.
- The anchor Packet Forwarding Engine is **pfe-1/0/0** and the anchor services PIC is **ms-5/0/0**.
- The S1-U interface uses **ge-0/0/0** and has IP address **10.44.0.1/16**
- The S5 interface uses **ge-0/0/1** and has IP address **10.5.0.1/16**
- The S11 interface uses **ge-0/0/2** and has IP address **10.2.2.1/16**

### Configuration

- [Configuring the Chassis on page 703](#)
- [Configuring the IPv4 Interfaces on page 704](#)
- [Configuring Offline Charging on page 704](#)

- [Configuring System Anchors on page 706](#)
- [Configuring GTP Services on page 707](#)

### Configuring the Chassis

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
load merge /etc/config/mobility-defaults.conf
set chassis fpc 1 pic 0 apply-groups mobility
set chassis fpc 1 forwarding-packages mobility sgw
set interfaces ms-5/0/0 unit 0 family inet address 10.4.1.1/32
set interfaces ge-0/0/0 unit 0 family inet address 10.44.0.1/16
set interfaces ge-0/0/1 unit 0 family inet address 10.5.0.1/16
set interfaces ge-0/0/2 unit 0 family inet address 10.2.2.0.1/16
set interfaces lo0 unit 0 family inet address 10.10.10.1/32
set interfaces lo0 unit 0 family inet address 127.0.0.1/32
set interfaces lo0 unit 0 family inet address 10.255.0.28/32 primary
```



**NOTE:** This configuration is for the S-GW only. Other statements are needed to make this a complete device configuration.

#### Step-by-Step Procedure

To configure the chassis:

1. Load and merge the default configuration file for the **mobility** group.

```
[edit]
user@sgw1# load merge /etc/config/mobility-defaults.conf
```

2. Configure the **mobility** group on the session DPC.

```
[edit]
user@sgw1# set chassis fpc 1 pic 0 apply-groups mobility
```



**NOTE:** You must include every services PIC configured with the **jservices-mobile** package at the **[edit unified-edge gateways sgw gateway-name system session-pics]** hierarchy level on the broadband gateway. If you do not include the services PIC as an anchor interface, then the services PIC will not be used by the broadband gateway.

3. Configure the interface DPC or MPC at the FPC level.

```
[edit]
user@sgw1# set chassis fpc 1 forwarding-packages mobility ggsn-pgw
```



**NOTE:** You must include every Packet Forwarding Engine configured with the `sgw` forwarding package at the `[edit unified-edge gateways sgw gateway-name system pfes]` hierarchy level on the broadband gateway. If you do not specify the Packet Forwarding Engine as an anchor interface, then the Packet Forwarding Engine will not be used by the broadband gateway.

---

4. Configure the Multiservices PIC interface.

[edit]

```
user@sgw1# set interfaces ms-5/0/0 unit 0 family inet address 10.10.10.1/32
```

5. Configure loopback interfaces.

[edit]

```
user@sgw1# set interfaces lo0 unit 0 family inet address 10.10.10.1/32
```

```
user@sgw1# set interfaces lo0 unit 0 family inet address 127.0.0.1/32
```

```
user@sgw1# set interfaces lo0 unit 0 family inet address 10.255.0.28/32 primary
```

---

### Configuring the IPv4 Interfaces

---

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

[edit]

```
set interfaces ge-0/0/0 unit 0 family inet address 10.44.0.1/16 description S1-U interface
```

```
set interfaces ge-0/0/1 unit 0 family inet address 10.5.0.1/16 description S5 interface
```

```
set interfaces ge-0/0/2 unit 0 family inet address 10.2.2.1/16 description S11 interface
```

#### Step-by-Step Procedure

To configure the IPv4 interfaces:

1. Configure IPv4 interfaces for the S1-U interface.

[edit]

```
user@sgw1# set interfaces ge-0/0/0 unit 0 family inet address 10.44.0.1/16  
description S1-U interface
```

2. Configure IPv4 interfaces for the S5 interface.

[edit]

```
user@sgw1# set interfaces ge-0/0/1 unit 0 family inet address 10.5.0.1/16 description  
S5 interface
```

3. Configure IPv4 interfaces for the S11 interface.

[edit]

```
user@sgw1# set interfaces ge-0/0/2 unit 0 family inet address 10.2.2.1/16 description  
S11 interface
```

---

### Configuring Offline Charging

---

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```

[edit]
set unified-edge gateways sgw SGW-MBG1 idle-mode-buffering
set unified-edge gateways sgw SGW-MBG1 charging trigger-profiles s_tp offline volume-limit
  1024
set unified-edge gateways sgw SGW-MBG1 charging trigger-profiles s_tp offline volume-limit
  direction both
set unified-edge gateways sgw SGW-MBG1 charging transport-profiles p_tsp offline
  charging-gateways cdr-release r8
set unified-edge gateways sgw SGW-MBG1 charging transport-profiles p_tsp offline
  charging-gateways peer-order peer p_cfg
set unified-edge gateways sgw SGW-MBG1 charging transport-profiles p_tsp offline
  charging-gateways switch-back-time 36
set unified-edge gateways sgw SGW-MBG1 charging charging-profiles p_juniper profile-id
  1
set unified-edge gateways sgw SGW-MBG1 charging charging-profiles p_juniper
  transport-profile p_tsp
set unified-edge gateways sgw SGW-MBG1 charging charging-profiles p_juniper
  trigger-profile s_tp
set unified-edge gateways sgw SGW-MBG1 charging gtp transport-protocol tcp
set unified-edge gateways sgw SGW-MBG1 charging gtp version v0
set unified-edge gateways sgw SGW-MBG1 charging gtp header-type long
set unified-edge gateways sgw SGW-MBG1 charging gtp peer p_cfg
  destination-ipv4-address 10.42.0.2
set unified-edge gateways sgw SGW-MBG1 charging gtp peer p_cfg source-interface
  ms-5/0/0,0
set unified-edge gateways sgw SGW-MBG1 charging gtp peer p_cfg source-interface
  ipv4-address 10.10.10.1
set unified-edge gateways sgw SGW-MBG1 charging gtp peer p_cfg destination-port 3386
set unified-edge gateways sgw SGW-MBG1 charging gtp peer p_cfg transport-protocol
  tcp
set unified-edge gateways sgw SGW-MBG1 charging gtp peer p_cfg n3-requests 1
set unified-edge gateways sgw SGW-MBG1 charging gtp peer p_cfg t3-response 3
set unified-edge gateways sgw SGW-MBG1 charging gtp peer p_cfg header-type long
set unified-edge gateways sgw SGW-MBG1 charging gtp peer p_cfg pending-queue-size
  1000
set unified-edge gateways sgw SGW-MBG1 charging global-profile default-profile p_juniper
set unified-edge gateways sgw SGW-MBG1 charging global-profile profile-selection-order
  static

```

### Step-by-Step Procedure

To configure the offline charging profile:

1. Configure charging for the S-GW called SGW-MBG1.  

```

[edit]
user@sgw1# edit unified-edge gateways sgw SGW-MBG1 charging

```
2. Specify the global GTP Prime properties to transmit CDRs to the external charging gateway.  

```

[edit unified-edge gateways sgw SGW-MBG1 charging]
user@sgw1# set gtp transport-protocol tcp
user@sgw1# set gtp version v0
user@sgw1# set gtp header-type long

```
3. Specify the GTP Prime properties for the GTP Prime peers.  

```

[edit unified-edge gateways sgw SGW-MBG1 charging]

```

```
user@sgw1# set gtp peer p_cgf destination-ipv4-address 10.42.0.2
user@sgw1# set gtp peer p_cgf source-interface ms-5/0/0.0
user@sgw1# set gtp peer p_cgf source-interface ipv4-address 10.10.10.1
user@sgw1# set gtp peer p_cgf destination-port 3386
user@sgw1# set gtp peer p_cgf transport-protocol tcp
user@sgw1# set gtp peer p_cgf n3-requests 1
user@sgw1# set gtp peer p_cgf t3-response 3
user@sgw1# set gtp peer p_cgf header-type long
user@sgw1# set gtp peer p_cgf pending-queue-size 1000
```

4. Configure idle-mode buffering for the S-GW.

```
[edit unified-edge gateways sgw SGW-MBG1 ]
user@sgw1# set idle-mode-buffering
```

5. Configure the transport, trigger, and global profiles referenced by the charging profile for offline charging.

```
[edit unified-edge gateways sgw SGW-MBG1 charging]
user@sgw1# set transport-profiles p_tsp offline charging-gateways cdr-release r8
user@sgw1# set transport-profiles p_tsp offline charging-gateways peer-order peer
p_cgf
user@sgw1# set transport-profiles p_tsp offline charging-gateways peer-order peer
p_cfg
user@sgw1# set transport-profiles p_tsp offline charging-gateways switch-back-time
36
user@sgw1# set trigger-profiles s_tp offline volume-limit 1024
user@sgw1# set trigger-profiles s_tp offline volume-limit direction both
```

6. Configure the charging profiles.

```
[edit unified-edge gateways sgw SGW-MBG1 charging]
user@sgw1# set charging-profiles p_juniper profile-id 1
user@sgw1# set charging-profiles p_juniper transport-profile p_cfg
user@sgw1# set charging-profiles p_juniper trigger-profile s_tp
```

---

### Configuring System Anchors

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge gateways sgw SGW-MBG1 system pfes interface pfe-1/0/0
set unified-edge gateways sgw SGW-MBG1 system session-pics interface ms-5/0/0
```

**Step-by-Step Procedure** To configure the anchor Packet Forwarding Engine and services PIC:

1. Configure the anchor Packet Forwarding Engine.

```
[edit unified-edge gateways sgw SGW-MBG1 system]
user@sgw1# set pfes interface pfe-1/0/0
```

2. Configure the anchor services PIC.

```
[edit unified-edge gateways sgw SGW-MBG1 system]
user@sgw1# set session-pics interface ms-5/0/0
```



### Configuring GTP Services

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge gateways sgw SGW-MBG1 gtp interface lo0.0
set unified-edge gateways sgw SGW-MBG1 gtp interface v4-address 10.10.10.1
set unified-edge gateways sgw SGW-MBG1 gtp path-management disable
set unified-edge gateways sgw SGW-MBG1 gtp control path-management disable
set unified-edge gateways sgw SGW-MBG1 gtp data path-management disable
set unified-edge gateways sgw SGW-MBG1 gtp s1u echo-interval 60
set unified-edge gateways sgw SGW-MBG1 gtp s5 echo-n3-requests 5
set unified-edge gateways sgw SGW-MBG1 gtp s5 echo-t3-response 30
set unified-edge gateways sgw SGW-MBG1 gtp s5 echo-interval 60
set unified-edge gateways sgw SGW-MBG1 gtp s11 echo-n3-requests 5
set unified-edge gateways sgw SGW-MBG1 gtp s11 echo-t3-response 30
```

**Step-by-Step Procedure** To configure GTP services:

1. Configure the GTP services for the S-GW called SGW-MBG1.

```
[edit]
user@sgw1# edit unified-edge gateways sgw SGW-MBG1 gtp
```

2. Configure GTP services for the S1-U, S5, and S11 interfaces with path management disabled. The same address must be specified for all addresses.

```
[edit unified-edge gateways sgw SGW-MBG1 gtp]
user@sgw1# set interface lo0.0
user@sgw1# set interface v4-address 10.10.10.1
user@sgw1# set path-management disable
user@sgw1# set control path-management disable
user@sgw1# set data path-management disable
user@sgw1# set su1 echo-interval 60
user@sgw1# set s5 echo-interval 60
user@sgw1# set s5 echo-n3-requests 5
user@sgw1# set s5 echo-t3-response 30
user@sgw1# set s11 echo-n3-requests 5
user@sgw1# set s11 echo-t3-response 30
```

### Verification

#### Verifying Gateway Status

**Purpose** Verify the gateways for the broadband gateway.

**Action** user@pgw-sgw-1> **show unified-edge gateways brief**

Total number of configured gateways: 1

Gateway name: SGW-MBG1

Gateway type: ggsn-pgw

Gateway id: 1

**Meaning** The **show unified-edge gateways brief** command displays information about the configured gateways.

- Related Documentation**
- [Example: Configuring a Multigateway P-GW and S-GW on page 719](#)
  - [Example: Configuring a Collocated P-GW and S-GW on page 708](#)

---

## Example: Configuring a Collocated P-GW and S-GW

This example describes how to configure the MobileNext Broadband Gateway as a collocated Packet Data Network Gateway (P-GW) and Serving Gateway (S-GW) sharing a chassis. The emphasis is on P-GW and S-GW configuration, and does not include many other parameters that a full device configuration requires.

- [Requirements on page 708](#)
- [Overview on page 708](#)
- [Configuration on page 709](#)
- [Verification on page 719](#)

### Requirements

This example uses the following hardware and software components:

- Junos OS Release 11.4W
- Juniper Networks MobileNext Broadband Gateway

### Overview

This example describes how to configure the broadband gateway as a collocated P-GW (PGW-MBG1) and S-GW (SGW-MBG1). Both P-GW and S-GW use the same chassis, which is named **pgw-sgw-1**.

- For the S-GW portion of the broadband gateway:
  - The S1-U data, S5, and S11 control interface are in the main routing instance
  - The anchor Packet Forwarding Engines are **pfe-8/0/0**, **pfe-8/1/0**, **pfe-8/2/0**, **pfe-8/3/0**, **pfe-9/0/0**, **pfe-9/1/0**, **pfe-9/2/0**, and **pfe-9/3/0**
  - The anchor services PICs are **ms-0/0/0** and **ms-1/0/0**
  - The S1-U interface uses **ge-5/0/0** and has IP address **10.44.0.1/16**, and S-GW interface **lo0.0** with address **10.8.88.1**

- The S5 interface uses **ge-5/0/1** and has IP address **10.5.0.1/16**, and S-GW interface **lo0.0** with address **10.7.88.1**
- The S11 interface uses **ge-5/0/2** and has IP address **10.2.2.1/16**, and S-GW interface **lo0.0** with address **10.6.88.1**
- For the P-GW portion of the broadband gateway:
  - The Gn and Gi interfaces are in the main routing instance
  - The anchor Packet Forwarding Engines are **pfe-10/0/0**, **pfe-10/1/0**, **pfe-10/2/0**, **pfe-10/3/0**, **pfe-10/0/0**, **pfe-11/1/0**, **pfe-11/2/0**, and **pfe-11/3/0**
  - The anchor services PICs are **ms-0/1/0** and **ms-1/1/0**
  - Two APNs (**APN1** and **APN2**) are configured to use **mif.0** and **mif.1** respectively, and **lo0.0** address **10.9.88.1**

## Configuration

To configure a collocated P-GW and S-GW, perform these tasks:

- [Configuring the Chassis on page 709](#)
- [Configuring Charging for the P-GW on page 711](#)
- [Configuring Charging for the S-GW on page 713](#)
- [Configuring System Anchors for the Broadband Gateway S-GW and P-GW on page 715](#)
- [Configuring GTP Services for the P-GW and S-GW on page 716](#)
- [Configure the APNs for the P-GW on page 717](#)

### Configuring the Chassis

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
load merge /etc/config/mobility-defaults.conf
set chassis fpc 0 pic 0 apply-groups mobility
set chassis fpc 0 pic 1 apply-groups mobility
set chassis fpc 1 pic 0 apply-groups mobility
set chassis fpc 1 pic 1 apply-groups mobility
set chassis fpc 5 forwarding-packages mobility sgw
set chassis fpc 7 forwarding-packages mobility sgw
set chassis fpc 8 forwarding-packages mobility sgw
set chassis fpc 9 forwarding-packages mobility sgw
set chassis fpc 10 forwarding-packages mobility ggsn-pgw
set chassis fpc 11 forwarding-packages mobility ggsn-pgw
set interfaces ms-0/0/0 unit 0 family inet description Session PIC for S-GW
set interfaces ms-0/0/0 unit 16000 family inet description Reserved mobile interface
set interfaces ms-0/1/0 unit 0 family inet description Session PIC for P-GW
set interfaces ms-0/1/0 unit 16000 family inet description Reserved mobile interface
set interfaces ms-1/0/0 unit 0 family inet description Session PIC for S-GW
set interfaces ms-1/0/0 unit 16000 family inet description Reserved mobile interface
set interfaces ms-1/1/0 unit 0 family inet description Session PIC for S-GW
set interfaces ms-1/1/0 unit 16000 family inet description Reserved mobile interface
```

```
set interfaces ge-5/0/0 unit 0 family inet address 10.44.0.1/16
set interfaces ge-5/0/1 unit 0 family inet address 10.5.0.1/16
set interfaces ge-5/0/2 unit 0 family inet address 10.2.2.1/16
set interfaces xe-10/3/1 unit 0 family inet address 10.3.1.1/24
set interfaces xe-10/3/2 unit 0 family inet address 10.3.2.1/24
set interfaces lo0 unit 0 family inet address 10.6.88.1/32
set interfaces lo0 unit 0 family inet address 10.7.88.1/32
set interfaces lo0 unit 0 family inet address 10.8.88.1/32
set interfaces lo0 unit 0 family inet address 10.9.88.1/32
```



**NOTE:** This configuration is for the S-GW and P-GW only. Other statements are needed to make this a complete device configuration.

#### Step-by-Step Procedure

To configure the chassis:

1. Load and merge the default configuration file for the **mobility** group.

[edit]

```
user@pgw-sgw-1# load merge /etc/config/mobility-defaults.conf
```

2. Configure the **mobility** group on the session DPC.

[edit]

```
user@pgw-sgw-1# set chassis fpc 0 pic 0 apply-groups mobility
user@pgw-sgw-1# set chassis fpc 0 pic 1 apply-groups mobility
user@pgw-sgw-1# set chassis fpc 1 pic 0 apply-groups mobility
user@pgw-sgw-1# set chassis fpc 1 pic 1 apply-groups mobility
```



**NOTE:** You must include every services PIC configured with the **jservices-mobile** package at the [edit unified-edge gateways sgw *gateway-name* system anchor-spics] hierarchy level on the broadband gateway. If you do not include the services PIC as an anchor interface, then the services PIC will not be used by the broadband gateway.

3. Configure the interface DPC or MPC at the FPC level.

[edit]

```
user@pgw-sgw-1# set chassis fpc 5 forwarding-packages mobility sgw
user@pgw-sgw-1# set chassis fpc 7 forwarding-packages mobility sgw
user@pgw-sgw-1# set chassis fpc 8 forwarding-packages mobility sgw
user@pgw-sgw-1# set chassis fpc 9 forwarding-packages mobility sgw
user@pgw-sgw-1# set chassis fpc 10 forwarding-packages mobility ggsn-pgw
user@pgw-sgw-1# set chassis fpc 11 forwarding-packages mobility ggsn-pgw
```



**NOTE:** You must include every Packet Forwarding Engine configured with the `sgw` or `ggsn-pgw` forwarding package at the `[edit unified-edge gateways sgw gateway-name system anchor-pfes]` or `[edit unified-edge gateways ggsn-pgw gateway-name system anchor-pfes]` hierarchy level on the broadband gateway. If you do not specify the Packet Forwarding Engine as an anchor interface, then the Packet Forwarding Engine will not be used by the broadband gateway.

4. Configure the Multiservices PIC interfaces.

```
[edit]
user@pgw-sgw-1# set interfaces ms-0/0/0 unit 0 family inet description Session
PIC for S-GW
user@pgw-sgw-1# set interfaces ms-0/0/0 unit 16000 family inet description
Reserved mobile interface
user@pgw-sgw-1# set interfaces ms-0/1/0 unit 0 family inet description Session
PIC for P-GW
user@pgw-sgw-1# set interfaces ms-0/1/0 unit 16000 family inet description
Reserved mobile interface
user@pgw-sgw-1# set interfaces ms-1/0/0 unit 0 family inet description Session
PIC for S-GW
user@pgw-sgw-1# set interfaces ms-1/0/0 unit 16000 family inet description
Reserved mobile interface
user@pgw-sgw-1# set interfaces ms-1/1/0 unit 0 family inet description Session
PIC for P-GW
user@pgw-sgw-1# set interfaces ms-1/1/0 unit 16000 family inet description
Reserved mobile interface
```

5. Configure physical interfaces.

```
user@pgw-sgw-1# set interfaces ge-5/0/0 unit 0 family inet address 10.44.0.1/16
description S1-U
user@pgw-sgw-1# set interfaces ge-5/0/1 unit 0 family inet address 10.5.0.1/16
description S5
user@pgw-sgw-1# set interfaces ge-5/0/2 unit 0 family inet address 10.2.2.1/16
description S11
user@pgw-sgw-1# set interfaces xe-10/3/1 unit 0 family inet address 10.3.1.1/16
user@pgw-sgw-1# set interfaces xe-10/3/2 unit 0 family inet address 10.3.1.2/16
```

6. Configure loopback interfaces.

```
[edit]
user@pgw-sgw-1# set interfaces lo0 unit 0 family inet address 10.6.88.1/32
user@pgw-sgw-1# set interfaces lo0 unit 0 family inet address 10.7.88.1/32
user@pgw-sgw-1# set interfaces lo0 unit 0 family inet address 10.8.88.1/32
user@pgw-sgw-1# set interfaces lo0 unit 0 family inet address 10.9.88.1/32
```

### Configuring Charging for the P-GW

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
```

```

set unified-edge gateways ggsn-pgw PGW-MBG1 charging cdr-profiles cdr_p
  enable-reduced-partial-cdrs
set unified-edge gateways ggsn-pgw PGW-MBG1 charging cdr-profiles cdr_p
  exclude-attributes serving-node-plmn-identifier
set unified-edge gateways ggsn-pgw PGW-MBG1 charging trigger-profiles p_tp offline
  time-limit 600
set unified-edge gateways ggsn-pgw PGW-MBG1 charging transport-profiles pgw_tsp
  offline charging-gateways cdr-release r8
set unified-edge gateways ggsn-pgw PGW-MBG1 charging transport-profiles pgw_tsp
  offline charging-gateways peer-order peer pgw_cfg
set unified-edge gateways ggsn-pgw PGW-MBG1 charging transport-profiles pgw_tsp
  offline charging-gateways switch-back-time 36
set unified-edge gateways ggsn-pgw PGW-MBG1 charging charging-profiles jnpr-1 profile-id
  1
set unified-edge gateways ggsn-pgw PGW-MBG1 charging charging-profiles jnpr-1
  transport-profile pgw_tsp
set unified-edge gateways ggsn-pgw PGW-MBG1 charging charging-profiles jnpr-1
  cdr-profile cdr_p
set unified-edge gateways ggsn-pgw PGW-MBG1 charging charging-profiles jnpr-1
  trigger-profile p_tp
set unified-edge gateways ggsn-pgw PGW-MBG1 charging gtp transport-protocol tcp
set unified-edge gateways ggsn-pgw PGW-MBG1 charging gtp version v2
set unified-edge gateways ggsn-pgw PGW-MBG1 charging gtp header-type long
set unified-edge gateways ggsn-pgw PGW-MBG1 charging gtp peer my_cfg
  destination-ipv4-address 10.3.3.3
set unified-edge gateways ggsn-pgw PGW-MBG1 charging gtp peer my_cfg
  source-interface lo0.0
set unified-edge gateways ggsn-pgw PGW-MBG1 charging gtp peer my_cfg
  source-interface ipv4-address 10.9.88.1
set unified-edge gateways ggsn-pgw PGW-MBG1 charging gtp peer my_cfg
  destination-port 3386
set unified-edge gateways ggsn-pgw PGW-MBG1 charging gtp peer my_cfg
  transport-protocol udp
set unified-edge gateways ggsn-pgw PGW-MBG1 charging gtp peer my_cfg n3-requests
  1
set unified-edge gateways ggsn-pgw PGW-MBG1 charging gtp peer my_cfg t3-response
  5
set unified-edge gateways ggsn-pgw PGW-MBG1 charging gtp peer my_cfg header-type
  short
set unified-edge gateways ggsn-pgw PGW-MBG1 charging gtp peer my_cfg
  pending-queue-size 1000

```

#### Step-by-Step Procedure

To configure the charging parameters:

1. Configure charging for the P-GW called PGW-MBG1.  

```

[edit]
user@pgw-sgw-1# edit unified-edge gateways ggsn-pgw PGW-MBG1 charging

```
2. Specify the global GTP Prime properties to transmit CDRs to the external charging gateway.  

```

[edit unified-edge gateways ggsn-pgw PGW-MBG1 charging]
user@pgw-sgw-1# set gtp transport-protocol tcp
user@pgw-sgw-1# set gtp version v2
user@pgw-sgw-1# set gtp header-type long

```

- Specify the GTP Prime properties for the GTP Prime peers.

```
[edit unified-edge gateways ggsn-pgw PGW-MBG1 charging]
user@pgw-sgw-1# set gtp peer my_cgf destination-ipv4-address 10.3.3.3
user@pgw-sgw-1# set gtp peer my_cgf source-interface lo0.0
user@pgw-sgw-1# set gtp peer my_cgf source-interface ipv4-address 10.9.88.1
user@pgw-sgw-1# set gtp peer my_cgf destination-port 3386
user@pgw-sgw-1# set gtp peer my_cgf transport-protocol udp
user@pgw-sgw-1# set gtp peer my_cgf n3-requests 1
user@pgw-sgw-1# set gtp peer my_cgf t3-response 5
user@pgw-sgw-1# set gtp peer my_cgf header-type short
user@pgw-sgw-1# set gtp peer my_cgf pending-queue-size 1000
```

- Configure the transport, trigger, and CDR profiles referenced by the charging profile for offline charging.

```
[edit unified-edge gateways ggsn-pgw PGW-MBG1 charging]
user@pgw-sgw-1# set cdr-profiles cdr_p enable-reduced-partial-cdrs
user@pgw-sgw-1# set cdr-profiles cdr_p exclude-attributes
    serving-node-plmn-identifier
user@pgw-sgw-1# set trigger-profiles p_tp offline time-limit 600
user@pgw-sgw-1# set transport-profiles pgw_tsp offline charging-gateways
    cdr-release r8
user@pgw-sgw-1# set transport-profiles pgw_tsp offline charging-gateways
    peer-order peer pgw_cfg
user@pgw-sgw-1# set transport-profiles pgw_tsp offline charging-gateways
    switch-back-time 36
```

- Configure the charging profiles.

```
[edit unified-edge gateways ggsn-sgw PGW-MBG1 charging]
user@pgw-sgw-1# set charging-profiles jnpr-1 profile-id 1
user@pgw-sgw-1# set charging-profiles jnpr-1 transport-profile pgw_tsp
user@pgw-sgw-1# set charging-profiles jnpr-1 cdr-profile cdr_p
user@pgw-sgw-1# set charging-profiles jnpr-1 trigger-profile p_tp
```

### Configuring Charging for the S-GW

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge gateways sgw SGW-MBG1 idle-mode-buffering
set unified-edge gateways sgw SGW-MBG1 charging trigger-profiles s_tp offline volume-limit
    1024
set unified-edge gateways sgw SGW-MBG1 charging trigger-profiles s_tp offline volume-limit
    direction both
set unified-edge gateways sgw SGW-MBG1 charging transport-profiles p_tsp offline
    charging-gateways cdr-release r8
set unified-edge gateways sgw SGW-MBG1 charging transport-profiles p_tsp offline
    charging-gateways peer-order peer p_cfg
set unified-edge gateways sgw SGW-MBG1 charging transport-profiles p_tsp offline
    charging-gateways switch-back-time 36
set unified-edge gateways sgw SGW-MBG1 charging charging-profiles p_juniper profile-id
    1
set unified-edge gateways sgw SGW-MBG1 charging charging-profiles p_juniper
    transport-profile p_tsp
```

```
set unified-edge gateways sgw SGW-MBG1 charging charging-profiles p_juniper
trigger-profile s_tp
set unified-edge gateways sgw SGW-MBG1 charging gtp transport-protocol tcp
set unified-edge gateways sgw SGW-MBG1 charging gtp version v0
set unified-edge gateways sgw SGW-MBG1 charging gtp header-type long
set unified-edge gateways sgw SGW-MBG1 charging gtp peer p_cfg
destination-ipv4-address 10.42.0.2
set unified-edge gateways sgw SGW-MBG1 charging gtp peer p_cfg source-interface
lo0.0
set unified-edge gateways sgw SGW-MBG1 charging gtp peer p_cfg source-interface
ipv4-address 10.6.88.1
set unified-edge gateways sgw SGW-MBG1 charging gtp peer p_cfg destination-port 3386
set unified-edge gateways sgw SGW-MBG1 charging gtp peer p_cfg transport-protocol
tcp
set unified-edge gateways sgw SGW-MBG1 charging gtp peer p_cfg n3-requests 1
set unified-edge gateways sgw SGW-MBG1 charging gtp peer p_cfg t3-response 3
set unified-edge gateways sgw SGW-MBG1 charging gtp peer p_cfg header-type long
set unified-edge gateways sgw SGW-MBG1 charging gtp peer p_cfg pending-queue-size
1000
set unified-edge gateways sgw SGW-MBG1 charging global-profile default-profile p_juniper
set unified-edge gateways sgw SGW-MBG1 charging global-profile profile-selection-order
static
```

**Step-by-Step  
Procedure**

To configure the offline charging profile:

1. Configure charging for the S-GW called SGW-MBG1.

```
[edit]
user@pgw-sgw-1# edit unified-edge gateways sgw SGW-MBG1 charging
```

2. Specify the global GTP Prime properties to transmit CDRs to the external charging gateway.

```
[edit unified-edge gateways sgw SGW-MBG1 charging]
user@pgw-sgw-1# set gtp transport-protocol tcp
user@pgw-sgw-1# set gtp version v0
user@pgw-sgw-1# set gtp header-type long
```

3. Specify the GTP Prime properties for the GTP Prime peers.

```
[edit unified-edge gateways sgw SGW-MBG1 charging]
user@pgw-sgw-1# set gtp peer p_cfg destination-ipv4-address 10.42.0.2
user@pgw-sgw-1# set gtp peer p_cfg source-interface lo0.0
user@pgw-sgw-1# set gtp peer p_cfg source-interface ipv4-address 10.6.88.1
user@pgw-sgw-1# set gtp peer p_cfg destination-port 3386
user@pgw-sgw-1# set gtp peer p_cfg transport-protocol tcp
user@pgw-sgw-1# set gtp peer p_cfgfw n3-requests 1
user@pgw-sgw-1# set gtp peer p_cfgfw t3-response 3
user@pgw-sgw-1# set gtp peer p_cfgfw header-type long
user@pgw-sgw-1# set gtp peer p_cfgfw pending-queue-size 1000
```

4. Configure idle-mode buffering for the S-GW.

```
[edit unified-edge gateways sgw SGW-MBG1 ]
user@pgw-sgw-1# set idle-mode-buffering
```

5. Configure the transport, trigger, and global profiles referenced by the charging profile for offline charging.



```
[edit unified-edge gateways sgw SGW-MBG1 charging]
user@pgw-sgw-1# set transport-profiles p_tsp offline charging-gateways cdr-release
r8
user@pgw-sgw-1# set transport-profiles p_tsp offline charging-gateways peer-order
peer p_cfg
user@pgw-sgw-1# set transport-profiles p_tsp offline charging-gateways peer-order
peer p_cfg
user@pgw-sgw-1# set transport-profiles p_tsp offline charging-gateways
switch-back-time 36
user@pgw-sgw-1# set trigger-profiles s_tp offline volume-limit 1024
user@pgw-sgw-1# set trigger-profiles s_tp offline volume-limit direction both
```

6. Configure the charging profile.

```
[edit unified-edge gateways sgw SGW-MBG1 charging]
user@pgw-sgw-1# set charging-profiles p_juniper profile-id 1
user@pgw-sgw-1# set charging-profiles p_juniper transport-profile p_cfg
user@pgw-sgw-1# set charging-profiles p_juniper trigger-profile s_tp
```

### Configuring System Anchors for the Broadband Gateway S-GW and P-GW

**CLI Quick  
Configuration**

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge gateways ggsn-pgw PGW-MBG1 system anchor-pfes interface pfe-10/0/0
set unified-edge gateways ggsn-pgw PGW-MBG1 system anchor-pfes interface pfe-10/1/0
set unified-edge gateways ggsn-pgw PGW-MBG1 system anchor-pfes interface pfe-10/2/0
set unified-edge gateways ggsn-pgw PGW-MBG1 system anchor-pfes interface pfe-10/3/0
set unified-edge gateways ggsn-pgw PGW-MBG1 system anchor-pfes interface pfe-11/0/0
set unified-edge gateways ggsn-pgw PGW-MBG1 system anchor-pfes interface pfe-11/1/0
set unified-edge gateways ggsn-pgw PGW-MBG1 system anchor-pfes interface pfe-11/2/0
set unified-edge gateways ggsn-pgw PGW-MBG1 system anchor-pfes interface pfe-11/3/0
set unified-edge gateways ggsn-pgw PGW-MBG1 system anchor-spics interface ms-1/1/0
set unified-edge gateways ggsn-pgw PGW-MBG1 system anchor-spics interface ms-0/1/0
set unified-edge gateways sgw SGW-MBG1 system anchor-pfes interface pfe-8/0/0
set unified-edge gateways sgw SGW-MBG1 system anchor-pfes interface pfe-8/1/0
set unified-edge gateways sgw SGW-MBG1 system anchor-pfes interface pfe-8/2/0
set unified-edge gateways sgw SGW-MBG1 system anchor-pfes interface pfe-8/3/0
set unified-edge gateways sgw SGW-MBG1 system anchor-pfes interface pfe-9/0/0
set unified-edge gateways sgw SGW-MBG1 system anchor-pfes interface pfe-9/1/0
set unified-edge gateways sgw SGW-MBG1 system anchor-pfes interface pfe-9/2/0
set unified-edge gateways sgw SGW-MBG1 system anchor-pfes interface pfe-9/3/0
set unified-edge gateways sgw SGW-MBG1 system anchor-spics interface ms-0/0/0
set unified-edge gateways sgw SGW-MBG1 system anchor-spics interface ms-1/0/0
```

**Step-by-Step  
Procedure**

To configure the anchor Packet Forwarding Engines and services PICs:

1. Configure the anchor Packet Forwarding Engines for the P-GW.

```
[edit unified-edge gateways ggsn-pgw PGW-MBG1 system]
user@pgw-sgw-1# set anchor-pfes interface pfe-10/0/0
user@pgw-sgw-1# set anchor-pfes interface pfe-10/1/0
user@pgw-sgw-1# set anchor-pfes interface pfe-10/2/0
user@pgw-sgw-1# set anchor-pfes interface pfe-10/3/0
user@pgw-sgw-1# set anchor-pfes interface pfe-11/0/0
```

```
user@pgw-sgw-1# set anchor-pfes interface pfe-11/1/0
user@pgw-sgw-1# set anchor-pfes interface pfe-11/2/0
user@pgw-sgw-1# set anchor-pfes interface pfe-11/3/0
```

2. Configure the anchor services PIC for the P-GW.

```
[edit unified-edge gateways ggsn-pgw PGW-MBG1 system]
user@pgw-sgw-1# set anchor-spics interface ms-1/1/0
user@pgw-sgw-1# set anchor-spics interface ms-0/1/0
```

3. Configure the anchor Packet Forwarding Engines for the S-GW.

```
[edit unified-edge gateways sgw SGW-MBG1 system]
user@pgw-sgw-1# set anchor-pfes interface pfe-8/0/0
user@pgw-sgw-1# set anchor-pfes interface pfe-8/1/0
user@pgw-sgw-1# set anchor-pfes interface pfe-8/2/0
user@pgw-sgw-1# set anchor-pfes interface pfe-8/3/0
user@pgw-sgw-1# set anchor-pfes interface pfe-9/0/0
user@pgw-sgw-1# set anchor-pfes interface pfe-9/1/0
user@pgw-sgw-1# set anchor-pfes interface pfe-9/2/0
user@pgw-sgw-1# set anchor-pfes interface pfe-9/3/0
```

4. Configure the anchor services PIC for the S-GW.

```
[edit unified-edge gateways sgw SGW-MBG1 system]
user@pgw-sgw-1# set anchor-spics interface ms-0/0/0
user@pgw-sgw-1# set anchor-spics interface ms-1/0/0
```

---

### Configuring GTP Services for the P-GW and S-GW

---

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge gateways ggsn-pgw PGW-MBG1 gtp interface lo0.0
set unified-edge gateways ggsn-pgw PGW-MBG1 gtp interface v4-address 10.9.88.1
set unified-edge gateways ggsn-pgw PGW-MBG1 gtp n3-requests 5
set unified-edge gateways ggsn-pgw PGW-MBG1 gtp t3-response 3
set unified-edge gateways ggsn-pgw PGW-MBG1 gtp echo-interval 60
set unified-edge gateways ggsn-pgw PGW-MBG1 gtp path-management-disable
set unified-edge gateways ggsn-pgw PGW-MBG1 gtp echo-n3-requests 5
set unified-edge gateways sgw SGW-MBG1 gtp path-management-disable
set unified-edge gateways sgw SGW-MBG1 gtp control path-management-disable
set unified-edge gateways sgw SGW-MBG1 gtp data path-management-disable
set unified-edge gateways sgw SGW-MBG1 gtp s1u interface lo0.0
set unified-edge gateways sgw SGW-MBG1 gtp s1u interface v4-address 10.8.88.1
set unified-edge gateways sgw SGW-MBG1 gtp s5 interface lo0.0
set unified-edge gateways sgw SGW-MBG1 gtp s5 interface v4-address 10.7.88.1
set unified-edge gateways sgw SGW-MBG1 gtp s11 interface lo0.0
set unified-edge gateways sgw SGW-MBG1 gtp s11 interface v4-address 10.6.88.1
set unified-edge gateways sgw SGW-MBG1 gtp s11 n3-requests 5
set unified-edge gateways sgw SGW-MBG1 gtp s11 t3-response 5
```

#### Step-by-Step Procedure

To configure GTP services:

1. Configure the GTP services for the P-GW called PGW-MBG1.

```
[edit]
```

- ```
user@pgw-sgw-1# edit unified-edge gateways pgw PGW-MBG1 gtp
```
2. Configure GTP services for the P-GW interfaces with path management disabled.
 

```
[edit unified-edge gateways pgw PGW-MBG1 gtp]
user@pgw-sgw-1# set interface lo0.0
user@pgw-sgw-1# set interface v4-address 10.9.88.1
user@pgw-sgw-1# set n3-requests 5
user@pgw-sgw-1# set t3-response 3
user@pgw-sgw-1# set echo-interval 60
user@pgw-sgw-1# set path-management disable
user@pgw-sgw-1# set echo-n3-requests 5
```
  3. Configure the GTP services for the S-GW called SGW-MBG1.
 

```
[edit]
user@pgw-sgw-1# edit unified-edge gateways sgw SGW-MBG1 gtp
```
  4. Configure GTP services for the S1-U, S5, and S11 interfaces with path management disabled. The same address must be specified for all addresses.
 

```
[edit unified-edge gateways sgw SGW-MBG1 gtp]
user@pgw-sgw-1# set path-management disable
user@pgw-sgw-1# set control path-management disable
user@pgw-sgw-1# set data path-management disable
user@pgw-sgw-1# set s1u interface lo0.0
user@pgw-sgw-1# set s1u interface v4-address 10.8.88.1
user@pgw-sgw-1# set s5 interface lo0.0
user@pgw-sgw-1# set s5 interface v4-address 10.7.88.1
user@pgw-sgw-1# set s11 interface lo0.0
user@pgw-sgw-1# set s11 interface v4-address 10.6.88.1
user@pgw-sgw-1# set s11 n3-requests 5
user@pgw-sgw-1# set s11 t3-response 5
```

### Configure the APNs for the P-GW

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge gateways ggsn-pgw PGW-MBG1 apn-services apns APN1
set unified-edge gateways ggsn-pgw PGW-MBG1 apn-services apns APN1 apn-data-type
  ipv4
set unified-edge gateways ggsn-pgw PGW-MBG1 apn-services apns APN1 mobile interface
  mif.0
set unified-edge gateways ggsn-pgw PGW-MBG1 apn-services apns APN1
  address-assignment local
set unified-edge gateways ggsn-pgw PGW-MBG1 apn-services apns APN1 charging
  default-profile jnpr
set unified-edge gateways ggsn-pgw PGW-MBG1 apn-services apns APN1 dns-server
  primary-v4 10.10.20.120
set unified-edge gateways ggsn-pgw PGW-MBG1 apn-services apns APN1 dns-server
  secondary-v4 10.10.20.119
set unified-edge gateways ggsn-pgw PGW-MBG1 apn-services apns APN1 dns-server
  primary-v6 10:10:20::120
set unified-edge gateways ggsn-pgw PGW-MBG1 apn-services apns APN1 dns-server
  secondary-v6 10:10:20::120
```

```
set unified-edge gateways ggsn-pgw PGW-MBG1 apn-services apns APN1 nbns-server
primary-v4 192.168.23.23
set unified-edge gateways ggsn-pgw PGW-MBG1 apn-services apns APN1 nbns-server
secondary-v4 192.168.23.24
set unified-edge gateways ggsn-pgw PGW-MBG1 apn-services apns APN1 p-cscf 10:10:10::10
set unified-edge gateways ggsn-pgw PGW-MBG1 apn-services apns APN1 selection-mode
from-ms
set unified-edge gateways ggsn-pgw PGW-MBG1 apn-services apns APN2
set unified-edge gateways ggsn-pgw PGW-MBG1 apn-services apns APN2 apn-data-type
ipv4
set unified-edge gateways ggsn-pgw PGW-MBG1 apn-services apns APN2 mobile interface
mif.1
set unified-edge gateways ggsn-pgw PGW-MBG1 apn-services apns APN1
address-assignment local
set unified-edge gateways ggsn-pgw PGW-MBG1 apn-services apns APN1 charging
default-profile jnpr
set unified-edge gateways ggsn-pgw PGW-MBG1 apn-services apns APN1 dns-server
primary-v4 10.10.20.120
set unified-edge gateways ggsn-pgw PGW-MBG1 apn-services apns APN1 p-cscf 10:10:10::10
set unified-edge gateways ggsn-pgw PGW-MBG1 apn-services apns APN1 selection-mode
from-ms
```

**Step-by-Step  
Procedure**

To configure APNs for the P-GW called PGW-MBG1:

1. Configure APN1 for the P-GW called PGW-MBG1.

```
[edit]
user@pgw-sgw-1# edit unified-edge gateways pgw PGW-MBG1 apn-services apns
APN1
[edit unified-edge gateways pgw PGW-MBG1 apn-services apns APN1]
user@pgw-sgw-1# set apn-data-type ipv4
user@pgw-sgw-1# set mobile-interface mif.0
user@pgw-sgw-1# set address-assignment local
user@pgw-sgw-1# set charging default-profile jnpr
user@pgw-sgw-1# set charging dns-server primary-v4 10.10.20.119
user@pgw-sgw-1# set charging dns-server secondary-v4 10.10.20.120
user@pgw-sgw-1# set charging dns-server primary-v4 10:10:20::119
user@pgw-sgw-1# set charging dns-server secondary-v4 10:10:20::120
user@pgw-sgw-1# set charging nbns-server primary-v4 192.168.23.23
user@pgw-sgw-1# set charging nbns-server secondary-v4 192.168.23.24
user@pgw-sgw-1# set p-cscf 10:10:10::10
user@pgw-sgw-1# set selection-mode from-ms
```

2. Configure APN2 for the P-GW called PGW-MBG1.

```
[edit]
user@pgw-sgw-1# edit unified-edge gateways pgw PGW-MBG1 apn-services apns
APN2
[edit unified-edge gateways pgw PGW-MBG1 apn-services apns APN2]
user@pgw-sgw-1# set apn-data-type ipv4
user@pgw-sgw-1# set mobile-interface mif.0
user@pgw-sgw-1# set address-assignment local
user@pgw-sgw-1# set charging default-profile jnpr
user@pgw-sgw-1# set p-cscf 10:10:10::10
user@pgw-sgw-1# set selection-mode from-ms
```

## Verification

### Verifying Gateway Status

|                              |                                                                                                                                                                                                                                                               |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Purpose</b>               | Verify the gateways for the broadband gateway.                                                                                                                                                                                                                |
| <b>Action</b>                | <pre>user@pgw-sgw-1&gt; show unified-edge gateways brief</pre> <p>Total number of configured gateways: 2</p> <p>Gateway name: PGW-MBG1<br/>Gateway type: ggsn-pgw<br/>Gateway id: 1</p> <p>Gateway name: SGW-MBG1<br/>Gateway type: sgw<br/>Gateway id: 2</p> |
| <b>Meaning</b>               | The <b>show unified-edge gateways brief</b> command displays information about the configured gateways.                                                                                                                                                       |
| <b>Related Documentation</b> | <ul style="list-style-type: none"> <li>• <a href="#">Example: Configuring a Multigateway P-GW and S-GW on page 719</a></li> <li>• <a href="#">Example: Configuring a Standalone S-GW on page 702</a></li> </ul>                                               |

## Example: Configuring a Multigateway P-GW and S-GW

This example describes how to configure the MobileNext Broadband Gateway with multiple Packet Data Network Gateways (P-GWs) and Serving Gateways (S-GWs) sharing a chassis. The emphasis is on P-GW and S-GW configuration, and does not include many other parameters that a full device configuration requires.

- [Requirements on page 719](#)
- [Overview on page 719](#)
- [Configuration on page 720](#)
- [Verification on page 733](#)

## Requirements

This example uses the following hardware and software components:

- Junos OS Release 11.4W
- Juniper Networks MobileNext Broadband Gateway

## Overview

This example describes how to configure the broadband gateway as a multigateway P-GW (PGW1-MBG1 and PGW2-MBG1) and S-GW (SGW1-MBG1 and SGW2-MBG1). All P-GWs and S-GWs use the same chassis, which is named **pgw-sgw-1**.

- For the two S-GWs on the broadband gateway:
  - The S1-U data, S5, and S11 control interface are in the main routing instance
  - The anchor Packet Forwarding Engine for SGW1-MBG1 is **pfe-1/0/0** and the anchor Packet Forwarding Engine for SGW2-MBG1 is **pfe-1/2/0**
  - The anchor services PIC for SGW1-MBG1 is **ms-5/0/0** and the anchor services PIC for SGW2-MBG1 is **ms-5/1/0**
  - The loopback address (**lo0.0**) for SGW1-MBG1 is **10.11.11.11** and the loopback address for SGW2-MBG1 is **10.22.22.22**



**NOTE:** The physical interfaces for the S1-U, S5, and S11 interfaces are not listed. These interfaces are established at runtime in a heuristic manner.

---

- For the two P-GWs on the broadband gateway:
  - The Gn and Gi interfaces are in the main routing instance and determined by runtime heuristics
  - The anchor Packet Forwarding Engine for PGW1-MBG1 is **pfe-0/0/0** and the anchor Packet Forwarding Engine for PGW2-MBG1 is **pfe-0/2/0**
  - The anchor services PIC for PGW1-MBG1 is **ms-3/0/0** and the anchor services PIC for SGW2-MBG1 is **ms-3/1/0**
  - The APN (**APN1** on PGW1-MBG1) uses mobile interface **mif.3** and the APN (**APN2** on PGW2-MBG1) uses mobile interface **mif.4**

## Configuration

To configure multiple P-GWs and S-GWs on the broadband gateway, perform these tasks:

- [Configuring the Chassis on page 721](#)
- [Configuring Charging for the P-GWs on page 723](#)
- [Configuring Charging for the S-GWs on page 726](#)
- [Configuring System Anchors for the Broadband Gateway P-GWs Named PGW1-MBG1 and PGW2-MBG2 on page 729](#)
- [Configuring System Anchors for the Broadband Gateway S-GWs Named SGW1-MBG1 and SGW2-MBG1 on page 730](#)
- [Configuring GTP Services for the P-GWs Named PGW1-MBG1 and PGW2-MBG2 on page 731](#)
- [Configuring GTP Services for the S-GW Named SGW1-MBG1 and SGW2-MBG1 on page 732](#)
- [Configure the APNs for the P-GW on page 733](#)

### Configuring the Chassis

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
load merge /etc/config/mobility-defaults.conf
set chassis fpc 3 pic 0 apply-groups mobility
set chassis fpc 3 pic 1 apply-groups mobility
set chassis fpc 5 pic 0 apply-groups mobility
set chassis fpc 5 pic 1 apply-groups mobility
set chassis fpc 0 forwarding-packages mobility ggsn-pgw
set chassis fpc 1 forwarding-packages mobility sgw
set interfaces ms-3/0/0 unit 0 family inet description Session PIC for PGW1-MBG1
set interfaces ms-3/0/0 unit 0 family inet address 10.4.1.3/32
set interfaces ms-3/1/0 unit 0 family inet description Session PIC for PGW2-MBG1
set interfaces ms-3/1/0 unit 0 family inet address 10.4.1.4/32
set interfaces ms-5/0/0 unit 0 family inet description Session PIC for SGW1-MBG1
set interfaces ms-5/0/0 unit 0 family inet address 10.4.1.1/32
set interfaces ms-5/1/0 unit 0 family inet description Session PIC for SGW2-MBG1
set interfaces ms-5/1/0 unit 0 family inet address 10.4.1.2/32
set interfaces ge-1/0/0 unit 0 family inet address 10.45.0.1/16
set interfaces ge-1/0/1 unit 0 family inet address 10.55.0.1/16
set interfaces ge-1/0/2 unit 0 family inet address 10.66.2.1/16
set interfaces ge-1/0/3 unit 0 family inet address 10.77.2.1/16
set interfaces lo0 unit 0 family inet address 10.11.11.11/32
set interfaces lo0 unit 0 family inet address 10.22.22.22/32
set interfaces lo0 unit 0 family inet address 10.33.33.33/32
set interfaces lo0 unit 0 family inet address 10.44.44.44/32
```



**NOTE:** This configuration is for the S-GWs and P-GWs only. Other statements are needed to make this a complete device configuration.

**Step-by-Step Procedure** To configure the chassis:

1. Load and merge the default configuration file for the **mobility** group.

```
[edit]
user@pgw-sgw-1# load merge /etc/config/mobility-defaults.conf
```

2. Configure the **mobility** group on the session DPC.

```
[edit]
user@pgw-sgw-1# set chassis fpc 3 pic 0 apply-groups mobility
user@pgw-sgw-1# set chassis fpc 3 pic 1 apply-groups mobility
user@pgw-sgw-1# set chassis fpc 5 pic 0 apply-groups mobility
user@pgw-sgw-1# set chassis fpc 5 pic 1 apply-groups mobility
```



**NOTE:** You must include every services PIC configured with the `jservices-mobile` package at the `[edit unified-edge gateways sgw gateway-name system anchor-spics]` hierarchy level on the broadband gateway. If you do not include the services PIC as an anchor interface, then the services PIC will not be used by the broadband gateway.

3. Configure the interface DPC or MPC at the FPC level.

[edit]

```
user@pgw-sgw-1# set chassis fpc 0 forwarding-packages mobility sgw
user@pgw-sgw-1# set chassis fpc 1 forwarding-packages mobility ggsn-pgw
```



**NOTE:** You must include every Packet Forwarding Engine configured with the `sgw` or `ggsn-pgw` forwarding package at the `[edit unified-edge gateways sgw gateway-name system anchor-pfes]` or `[edit unified-edge gateways ggsn-pgw gateway-name system anchor-pfes]` hierarchy level on the broadband gateway. If you do not specify the Packet Forwarding Engine as an anchor interface, then the Packet Forwarding Engine will not be used by the broadband gateway.

4. Configure the Multiservices PIC interfaces.

[edit]

```
user@pgw-sgw-1# set interfaces ms-3/0/0 unit 0 family inet description Session
PIC for PGW1-MBG1
user@pgw-sgw-1# set interfaces ms-3/0/0 unit 0 family inet address 10.4.1.3/32
user@pgw-sgw-1# set interfaces ms-3/1/0 unit 0 family inet description Session
PIC for PGW2-MBG1
user@pgw-sgw-1# set interfaces ms-3/1/0 unit 0 family inet address 10.4.1.4/32
user@pgw-sgw-1# set interfaces ms-5/0/0 unit 0 family inet description Session
PIC for SGW1-MBG1
user@pgw-sgw-1# set interfaces ms-5/0/0 unit 0 family inet address 10.4.1.1/32
user@pgw-sgw-1# set interfaces ms-5/1/0 unit 0 family inet description Session
PIC for SGW1-MBG1
user@pgw-sgw-1# set interfaces ms-5/1/0 unit 0 family inet address 10.4.1.2/32
```

5. Configure physical interfaces.

```
user@pgw-sgw-1# set interfaces ge-1/0/0 unit 0 family inet address 10.45.0.1/16
user@pgw-sgw-1# set interfaces ge-1/0/1 unit 0 family inet address 10.55.0.1/16
user@pgw-sgw-1# set interfaces ge-1/0/2 unit 0 family inet address 10.66.2.1/16
user@pgw-sgw-1# set interfaces ge-1/0/3 unit 0 family inet address 10.77.2.1/16
```

6. Configure loopback interfaces.

[edit]

```
user@pgw-sgw-1# set interfaces lo0 unit 0 family inet address 10.11.11.11/32
user@pgw-sgw-1# set interfaces lo0 unit 0 family inet address 10.22.22.22/32
user@pgw-sgw-1# set interfaces lo0 unit 0 family inet address 10.33.33.33/32
user@pgw-sgw-1# set interfaces lo0 unit 0 family inet address 10.44.44.44/32
```



### Configuring Charging for the P-GWs

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging trigger-profiles p_tp exclude
  plmn-change
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging trigger-profiles p_tp exclude
  rat-change
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging trigger-profiles p_tp offline
  volume-limit 1024
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging trigger-profiles p_tp offline
  volume-limit direction both
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging transport-profiles p_tsp offline
  charging-gateways cdr-release r7
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging transport-profiles p_tsp offline
  charging-gateways peer-order peer p_cfg
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging transport-profiles p_tsp offline
  charging-gateways switch-back-time 36
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging charging-profiles p_juniper
  profile-id 1
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging charging-profiles p_juniper
  transport-profile p_tsp
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging charging-profiles p_juniper
  trigger-profile p_tp
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging gtp transport-protocol tcp
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging gtp version v0
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging gtp header-type long
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging gtp peer p_cfg
  destination-ipv4-address 10.2.2.2
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging gtp peer p_cfg source-interface
  ms-3/0/0.0
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging gtp peer p_cfg source-interface
  ipv4-address 10.4.1.3
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging gtp peer p_cfg destination-port
  3386
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging gtp peer p_cfg
  transport-protocol tcp
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging gtp peer p_cfg n3-requests
  1
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging gtp peer p_cfg t3-response
  5
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging gtp peer p_cfg header-type
  long
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging gtp peer p_cfg
  pending-queue-size 1000
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging global-profile default-profile
  p_juniper
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging global-profile
  profile-selection-order static

[edit]
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging trigger-profiles p_tp exclude
  plmn-change
```

```
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging trigger-profiles p_tp exclude
  rat-change
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging trigger-profiles p_tp offline
  volume-limit 1024
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging trigger-profiles p_tp offline
  volume-limit direction both
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging transport-profiles p_tsp offline
  charging-gateways cdr-release r7
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging transport-profiles p_tsp offline
  charging-gateways peer-order peer p_cfg
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging charging-profiles p_juniper
  profile-id 1
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging charging-profiles p_juniper
  transport-profile p_tsp
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging charging-profiles p_juniper
  trigger-profile p_tp
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging gtp transport-protocol tcp
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging gtp version v0
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging gtp header-type long
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging gtp peer p_cfg
  destination-ipv4-address 10.2.2.2
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging gtp peer p_cfg source-interface
  ms-3/1/0.0
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging gtp peer p_cfg source-interface
  ipv4-address 10.4.1.4
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging gtp peer p_cfg destination-port
  3386
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging gtp peer p_cfg
  transport-protocol tcp
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging gtp peer p_cfg n3-requests
  1
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging gtp peer p_cfg t3-response
  5
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging gtp peer p_cfg header-type
  long
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging gtp peer p_cfg
  pending-queue-size 1000
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging global-profile default-profile
  p_juniper
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging global-profile
  profile-selection-order static
```

**Step-by-Step  
Procedure**

To configure the charging parameters:

1. Configure charging for the P-GW called PGW1-MBG1.  
  
[edit]  
user@pgw-sgw-1# edit unified-edge gateways ggsn-pgw PGW1-MBG1 charging
2. Specify the global GTP Prime properties of PGW1- MBG1 to transmit CDRs to the external charging gateway.  
  
[edit unified-edge gateways ggsn-pgw PGW1-MBG1 charging]  
user@pgw-sgw-1# set gtp transport-protocol tcp  
user@pgw-sgw-1# set gtp version v0  
user@pgw-sgw-1# set gtp header-type long

3. Specify the GTP Prime properties of PGW1-MBG1 for the GTP Prime peers.

```
[edit unified-edge gateways ggsn-pgw PGW1-MBG1 charging]
user@pgw-sgw-1# set gtp peer p_cgf destination-ipv4-address 10.2.2.2
user@pgw-sgw-1# set gtp peer p_cgf source-interface ms-3/0/0.0
user@pgw-sgw-1# set gtp peer p_cgf source-interface ipv4-address 10.4.1.3
user@pgw-sgw-1# set gtp peer p_cgf destination-port 3386
user@pgw-sgw-1# set gtp peer p_cgf transport-protocol tcp
user@pgw-sgw-1# set gtp peer p_cgf version v0
user@pgw-sgw-1# set gtp peer p_cgf n3-requests 1
user@pgw-sgw-1# set gtp peer p_cgf t3-response 5
user@pgw-sgw-1# set gtp peer p_cgf header-type long
user@pgw-sgw-1# set gtp peer p_cgf pending-queue-size 1000
```

4. Configure the transport and profiles referenced by the charging profile of PGW1-MBG1 for offline charging.

```
[edit unified-edge gateways ggsn-pgw PGW1-MBG1 charging]
user@pgw-sgw-1# set trigger-profiles p_tp exclude plmn-change
user@pgw-sgw-1# set trigger-profiles p_tp exclude rat-change
user@pgw-sgw-1# set trigger-profiles p_tp offline volume-limit 1024
user@pgw-sgw-1# set trigger-profiles p_tp offline volume-limit direction both
user@pgw-sgw-1# set transport-profiles p_tsp offline charging-gateways cdr-release
r7
user@pgw-sgw-1# set transport-profiles p_tsp offline charging-gateways peer-order
peer p_cgf
user@pgw-sgw-1# set transport-profiles p_tsp offline charging-gateways
switch-back-time 36
```

5. Configure the charging and global profiles for PGW1-MBG1.

```
[edit unified-edge gateways ggsn-sgw PGW1-MBG1 charging]
user@pgw-sgw-1# set charging-profiles p_juniper profile-id 1
user@pgw-sgw-1# set charging-profiles p_juniper transport-profile p_tsp
user@pgw-sgw-1# set charging-profiles p_juniper trigger-profile p_tp
user@pgw-sgw-1# set charging-profiles p_juniper global-profile p_juniper
user@pgw-sgw-1# set charging-profiles p_juniper global-profile
profile-selection-order static
```

6. Configure charging for the P-GW called PGW2-MBG1.

```
[edit]
user@pgw-sgw-1# edit unified-edge gateways ggsn-pgw PGW2-MBG1 charging
```

7. Specify the global GTP Prime properties of PGW2-MBG1 to transmit CDRs to the external charging gateway.

```
[edit unified-edge gateways ggsn-pgw PGW2-MBG1 charging]
user@pgw-sgw-1# set gtp transport-protocol tcp
user@pgw-sgw-1# set gtp version v0
user@pgw-sgw-1# set gtp header-type long
```

8. Specify the GTP Prime properties of PGW2-MBG1 for the GTP Prime peers.

```
[edit unified-edge gateways ggsn-pgw PGW2-MBG1 charging]
user@pgw-sgw-1# set gtp peer p_cgf destination-ipv4-address 10.2.2.2
user@pgw-sgw-1# set gtp peer p_cgf source-interface ms-3/1/0.0
user@pgw-sgw-1# set gtp peer p_cgf source-interface ipv4-address 10.4.1.4
user@pgw-sgw-1# set gtp peer p_cgf destination-port 3386
user@pgw-sgw-1# set gtp peer p_cgf transport-protocol tcp
```

```

user@pgw-sgw-1# set gtp peer p_cfg version v0
user@pgw-sgw-1# set gtp peer p_cfg n3-requests 1
user@pgw-sgw-1# set gtp peer p_cfg t3-response 5
user@pgw-sgw-1# set gtp peer p_cfg header-type long
user@pgw-sgw-1# set gtp peer p_cfg pending-queue-size 1000

```

9. Configure the transport and profiles referenced by the charging profile of PGW2-MBG1 for offline charging.

```

[edit unified-edge gateways ggsn-pgw PGW2-MBG1 charging]
user@pgw-sgw-1# set trigger-profiles p_tp exclude plmn-change
user@pgw-sgw-1# set trigger-profiles p_tp exclude rat-change
user@pgw-sgw-1# set trigger-profiles p_tp offline volume-limit 1024
user@pgw-sgw-1# set trigger-profiles p_tp offline volume-limit direction both
user@pgw-sgw-1# set transport-profiles p_tsp offline charging-gateways cdr-release
r7
user@pgw-sgw-1# set transport-profiles p_tsp offline charging-gateways peer-order
peer p_cfg

```

10. Configure the charging and global profiles for PGW2-MBG1.

```

[edit unified-edge gateways ggsn-pgw PGW2-MBG1 charging]
user@pgw-sgw-1# set charging-profiles p_juniper profile-id 1
user@pgw-sgw-1# set charging-profiles p_juniper transport-profile p_tsp
user@pgw-sgw-1# set charging-profiles p_juniper trigger-profile p_tp
user@pgw-sgw-1# set charging-profiles p_juniper global-profile p_juniper
user@pgw-sgw-1# set charging-profiles p_juniper global-profile
profile-selection-order static

```

### Configuring Charging for the S-GWs

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```

[edit]
set unified-edge gateways sgw SGW1-MBG1 charging trigger-profiles s_tp offline
volume-limit 1024
set unified-edge gateways sgw SGW1-MBG1 charging trigger-profiles s_tp offline
volume-limit direction both
set unified-edge gateways sgw SGW1-MBG1 charging transport-profiles p_tsp offline
charging-gateways cdr-release r8
set unified-edge gateways sgw SGW1-MBG1 charging transport-profiles p_tsp offline
charging-gateways peer-order peer p_cfg
set unified-edge gateways sgw SGW1-MBG1 charging transport-profiles p_tsp offline
charging-gateways switch-back-time 36
set unified-edge gateways sgw SGW1-MBG1 charging charging-profiles p_juniper profile-id
1
set unified-edge gateways sgw SGW1-MBG1 charging charging-profiles p_juniper
transport-profile p_tsp
set unified-edge gateways sgw SGW1-MBG1 charging charging-profiles p_juniper
trigger-profile s_tp
set unified-edge gateways sgw SGW1-MBG1 charging gtp transport-protocol tcp
set unified-edge gateways sgw SGW1-MBG1 charging gtp version v0
set unified-edge gateways sgw SGW1-MBG1 charging gtp header-type long
set unified-edge gateways sgw SGW1-MBG1 charging gtp peer p_cfg
destination-ipv4-address 10.2.2.2

```

```

set unified-edge gateways sgw SGW1-MBG1 charging gtp peer p_cfg source-interface
  ms-5/0/0.0
set unified-edge gateways sgw SGW1-MBG1 charging gtp peer p_cfg source-interface
  ipv4-address 10.4.1.1
set unified-edge gateways sgw SGW1-MBG1 charging gtp peer p_cfg destination-port
  3386
set unified-edge gateways sgw SGW1-MBG1 charging gtp peer p_cfg transport-protocol
  tcp
set unified-edge gateways sgw SGW1-MBG1 charging gtp peer p_cfg version v0
set unified-edge gateways sgw SGW1-MBG1 charging gtp peer p_cfg n3-requests 1
set unified-edge gateways sgw SGW1-MBG1 charging gtp peer p_cfg t3-response 5
set unified-edge gateways sgw SGW1-MBG1 charging gtp peer p_cfg header-type long
set unified-edge gateways sgw SGW1-MBG1 charging gtp peer p_cfg pending-queue-size
  1000
set unified-edge gateways sgw SGW1-MBG1 charging global-profile default-profile p_juniper
set unified-edge gateways sgw SGW1-MBG1 charging global-profile profile-selection-order
  static

```

[edit]

```

set unified-edge gateways sgw SGW2-MBG1 charging trigger-profiles p_tp exclude
  plmn-change
set unified-edge gateways sgw SGW2-MBG1 charging trigger-profiles p_tp exclude
  rat-change
set unified-edge gateways sgw SGW2-MBG1 charging trigger-profiles s_tp offline
  volume-limit 1024
set unified-edge gateways sgw SGW2-MBG1 charging trigger-profiles s_tp offline
  volume-limit direction both
set unified-edge gateways sgw SGW2-MBG1 charging transport-profiles p_tsp offline
  charging-gateways cdr-release r8
set unified-edge gateways sgw SGW2-MBG1 charging transport-profiles p_tsp offline
  charging-gateways peer-order peer p_cgf
set unified-edge gateways sgw SGW2-MBG1 charging transport-profiles p_tsp offline
  charging-gateways switchback-time 36
set unified-edge gateways sgw SGW2-MBG1 charging charging-profiles p_juniper profile-id
  1
set unified-edge gateways sgw SGW2-MBG1 charging charging-profiles p_juniper
  transport-profile p_tsp
set unified-edge gateways sgw SGW2-MBG1 charging charging-profiles p_juniper
  trigger-profile s_tp
set unified-edge gateways sgw SGW2-MBG1 charging gtp transport-protocol tcp
set unified-edge gateways sgw SGW2-MBG1 charging gtp version v0
set unified-edge gateways sgw SGW2-MBG1 charging gtp header-type long
set unified-edge gateways sgw SGW2-MBG1 charging gtp peer p_cfg
  destination-ipv4-address 10.2.2.2
set unified-edge gateways sgw SGW2-MBG1 charging gtp peer p_cfg source-interface
  ms-5/1/0.0
set unified-edge gateways sgw SGW2-MBG1 charging gtp peer p_cfg source-interface
  ipv4-address 10.4.1.2
set unified-edge gateways sgw SGW2-MBG1 charging gtp peer p_cfg destination-port
  3386
set unified-edge gateways sgw SGW2-MBG1 charging gtp peer p_cfg transport-protocol
  tcp
set unified-edge gateways sgw SGW2-MBG1 charging gtp peer p_cfg version v0
set unified-edge gateways sgw SGW2-MBG1 charging gtp peer p_cfg n3-requests 1
set unified-edge gateways sgw SGW2-MBG1 charging gtp peer p_cfg t3-response 5

```

```
set unified-edge gateways sgw SGW2-MBG1 charging gtp peer p_cfg header-type long
set unified-edge gateways sgw SGW2-MBG1 charging gtp peer p_cfg pending-queue-size
1000
set unified-edge gateways sgw SGW2-MBG1 charging global-profile default-profile p_juniper
set unified-edge gateways sgw SGW2-MBG1 charging global-profile profile-selection-order
static
```

**Step-by-Step  
Procedure**

To configure the charging parameters:

1. Configure charging for the S-GW called SGW1-MBG1.  
  
[edit]  
user@pgw-sgw-1# edit unified-edge gateways sgw SGW1-MBG1 charging
2. Specify the global GTP Prime properties of SGW1- MBG1 to transmit CDRs to the external charging gateway.  
  
[edit unified-edge gateways sgw SGW1-MBG1 charging]  
user@pgw-sgw-1# set gtp transport-protocol tcp  
user@pgw-sgw-1# set gtp version v0  
user@pgw-sgw-1# set gtp header-type long
3. Specify the GTP Prime properties of SGW1-MBG1 for the GTP Prime peers.  
  
[edit unified-edge gateways sgw SGW1-MBG1 charging]  
user@pgw-sgw-1# set gtp peer p\_cfg destination-ipv4-address 10.2.2.2  
user@pgw-sgw-1# set gtp peer p\_cfg source-interface ms-5/0/0.0  
user@pgw-sgw-1# set gtp peer p\_cfg source-interface ipv4-address 10.4.1.1  
user@pgw-sgw-1# set gtp peer p\_cfg destination-port 3386  
user@pgw-sgw-1# set gtp peer p\_cfg transport-protocol tcp  
user@pgw-sgw-1# set gtp peer p\_cfg version v0  
user@pgw-sgw-1# set gtp peer p\_cfg n3-requests 1  
user@pgw-sgw-1# set gtp peer p\_cfg t3-response 5  
user@pgw-sgw-1# set gtp peer p\_cfg header-type long  
user@pgw-sgw-1# set gtp peer p\_cfg pending-queue-size 1000
4. Configure the transport and profiles referenced by the charging profile of SGW1-MBG1 for offline charging.  
  
[edit unified-edge gateways sgw SGW1-MBG1 charging]  
user@pgw-sgw-1# set trigger-profiles s\_tp offline volume-limit 1024  
user@pgw-sgw-1# set trigger-profiles s\_tp offline volume-limit direction both  
user@pgw-sgw-1# set transport-profiles p\_tsp offline charging-gateways cdr-release  
r8  
user@pgw-sgw-1# set transport-profiles p\_tsp offline charging-gateways peer-order  
peer p\_cfg  
user@pgw-sgw-1# set transport-profiles p\_tsp offline charging-gateways  
switch-back-time 36
5. Configure the charging and global profiles for SGW1-MBG1.  
  
[edit unified-edge gateways sgw SGW1-MBG1 charging]  
user@pgw-sgw-1# set charging-profiles p\_juniper profile-id 1  
user@pgw-sgw-1# set charging-profiles p\_juniper transport-profile p\_tsp  
user@pgw-sgw-1# set charging-profiles p\_juniper trigger-profile s\_tp  
user@pgw-sgw-1# set charging-profiles p\_juniper global-profile p\_juniper  
user@pgw-sgw-1# set charging-profiles p\_juniper global-profile  
profile-selection-order static

6. Configure charging for the S-GW called SGW2-MBG1.
 

```
[edit]
user@pgw-sgw-1# edit unified-edge gateways sgw SGW2-MBG1 charging
```
7. Specify the global GTP Prime properties of SGW2-MBG1 to transmit CDRs to the external charging gateway.
 

```
[edit unified-edge gateways sgw SGW2-MBG1 charging]
user@pgw-sgw-1# set gtp transport-protocol tcp
user@pgw-sgw-1# set gtp version v0
user@pgw-sgw-1# set gtp header-type long
```
8. Specify the GTP Prime properties of SGW2-MBG1 for the GTP Prime peers.
 

```
[edit unified-edge gateways sgw SGW2-MBG1 charging]
user@pgw-sgw-1# set gtp peer p_cgf destination-ipv4-address 10.2.2.2
user@pgw-sgw-1# set gtp peer p_cgf source-interface ms-5/1/0.0
user@pgw-sgw-1# set gtp peer p_cgf source-interface ipv4-address 10.4.1.2
user@pgw-sgw-1# set gtp peer p_cgf destination-port 3386
user@pgw-sgw-1# set gtp peer p_cgf transport-protocol tcp
user@pgw-sgw-1# set gtp peer p_cgf version v0
user@pgw-sgw-1# set gtp peer p_cgf n3-requests 1
user@pgw-sgw-1# set gtp peer p_cgf t3-response 5
user@pgw-sgw-1# set gtp peer p_cgf header-type long
user@pgw-sgw-1# set gtp peer p_cgf pending-queue-size 1000
```
9. Configure the transport and profiles referenced by the charging profile of SGW2-MBG1 for offline charging.
 

```
[edit unified-edge gateways sgw SGW2-MBG1 charging]
user@pgw-sgw-1# set trigger-profiles p_tp exclude plmn-change
user@pgw-sgw-1# set trigger-profiles p_tp exclude rat-change
user@pgw-sgw-1# set trigger-profiles p_tp offline volume-limit 1024
user@pgw-sgw-1# set trigger-profiles p_tp offline volume-limit direction both
user@pgw-sgw-1# set transport-profiles p_tsp offline charging-gateways cdr-release
r8
user@pgw-sgw-1# set transport-profiles p_tsp offline charging-gateways peer-order
peer p_cfg
user@pgw-sgw-1# set transport-profiles p_tsp offline charging-gateways
switch-back-time 36
```
10. Configure the charging and global profiles for SGW2-MBG1.
 

```
[edit unified-edge gateways sgw SGW2-MBG1 charging]
user@pgw-sgw-1# set charging-profiles p_juniper profile-id 1
user@pgw-sgw-1# set charging-profiles p_juniper transport-profile p_tsp
user@pgw-sgw-1# set charging-profiles p_juniper trigger-profile s_tp
user@pgw-sgw-1# set charging-profiles p_juniper global-profile p_juniper
user@pgw-sgw-1# set charging-profiles p_juniper global-profile
profile-selection-order static
```

### Configuring System Anchors for the Broadband Gateway P-GWs Named PGW1-MBG1 and PGW2-MBG2

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

[edit]

```
set unified-edge gateways ggsn-pgw PGW1-MBG1 system anchor-pfes interface pfe-0/0/0
set unified-edge gateways ggsn-pgw PGW2-MBG1 system anchor-pfes interface pfe-0/2/0
set unified-edge gateways ggsn-pgw PGW1-MBG1 system anchor-spics interface ms-3/0/0
set unified-edge gateways ggsn-pgw PGW1-MBG1 system anchor-spics interface ms-3/1/0
```

#### Step-by-Step Procedure

To configure the anchor Packet Forwarding Engines and services PICs for the P-GWs:

1. Configure the anchor Packet Forwarding Engine for PGW1-MBG1.

```
[edit unified-edge gateways ggsn-pgw PGW1-MBG1 system]
user@pgw-sgw-1# set anchor-pfes interface pfe-0/0/0
```

2. Configure the anchor Packet Forwarding Engine for PGW2-MBG1.

```
[edit unified-edge gateways ggsn-pgw PGW2-MBG1 system]
user@pgw-sgw-1# set anchor-pfes interface pfe-0/2/0
```

3. Configure the anchor services PIC for PGW1-MBG1.

```
[edit unified-edge gateways ggsn-pgw PGW1-MBG1 system]
user@pgw-sgw-1# set anchor-spics interface ms-3/0/0
```

4. Configure the anchor services PIC for PGW2-MBG1.

```
[edit unified-edge gateways ggsn-pgw PGW2-MBG1 system]
user@pgw-sgw-1# set anchor-spics interface ms-3/1/0
```

### Configuring System Anchors for the Broadband Gateway S-GWs Named SGW1-MBG1 and SGW2-MBG1

---

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

[edit]

```
set unified-edge gateways sgw SGW1-MBG1 system anchor-pfes interface pfe-1/0/0
set unified-edge gateways sgw SGW1-MBG1 system anchor-pfes interface pfe-1/2/0
set unified-edge gateways sgw SGW1-MBG1 system anchor-spics interface ms-5/0/0
set unified-edge gateways sgw SGW1-MBG1 system anchor-spics interface ms-5/1/0
```

#### Step-by-Step Procedure

To configure the anchor Packet Forwarding Engines and services PICs for the S-GWs:

1. Configure the anchor Packet Forwarding Engine for SGW1-MBG1.

```
[edit unified-edge gateways sgw SGW1-MBG1 system]
user@pgw-sgw-1# set anchor-pfes interface pfe-1/0/0
```

2. Configure the anchor Packet Forwarding Engine for SGW2-MBG1.

```
[edit unified-edge gateways sgw SGW2-MBG1 system]
user@pgw-sgw-1# set anchor-pfes interface pfe-1/2/0
```

3. Configure the anchor services PIC for SGW1-MBG1.

```
[edit unified-edge gateways sgw SGW1-MBG1 system]
user@pgw-sgw-1# set anchor-spics interface ms-5/0/0
```

4. Configure the anchor services PIC for SGW2-MBG1.

```
[edit unified-edge gateways sgw SGW2-MBG1 system]
```



```
user@pgw-sgw-1# set anchor-spics interface ms-5/1/0
```

### Configuring GTP Services for the P-GWs Named PGW1-MBG1 and PGW2-MBG2

#### CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge gateways ggsn-pgw PGW1-MBG1 gtp interface lo0.0
set unified-edge gateways ggsn-pgw PGW1-MBG1 gtp interface v4-address 10.33.33.33
set unified-edge gateways ggsn-pgw PGW1-MBG1 gtp n3-requests 5
set unified-edge gateways ggsn-pgw PGW1-MBG1 gtp t3-response 3
set unified-edge gateways ggsn-pgw PGW1-MBG1 gtp echo-interval 60
set unified-edge gateways ggsn-pgw PGW1-MBG1 gtp path-management enable
set unified-edge gateways ggsn-pgw PGW1-MBG1 gtp echo-n3-requests 5
set unified-edge gateways ggsn-pgw PGW1-MBG1 gtp echo-t3-response 30
set unified-edge gateways ggsn-pgw PGW2-MBG1 gtp interface lo0.0
set unified-edge gateways ggsn-pgw PGW2-MBG1 gtp interface v4-address 10.44.44.44
set unified-edge gateways ggsn-pgw PGW2-MBG1 gtp n3-requests 5
set unified-edge gateways ggsn-pgw PGW2-MBG1 gtp t3-response 3
set unified-edge gateways ggsn-pgw PGW2-MBG1 gtp echo-interval 60
set unified-edge gateways ggsn-pgw PGW2-MBG1 gtp path-management enable
set unified-edge gateways ggsn-pgw PGW2-MBG1 gtp echo-n3-requests 5
set unified-edge gateways ggsn-pgw PGW2-MBG1 gtp echo-t3-response 30
```

#### Step-by-Step Procedure

To configure GTP services:

1. Configure the GTP services for the P-GW called PGW1-MBG1.

```
[edit]
user@pgw-sgw-1# edit unified-edge gateways ggsn-pgw PGW1-MBG1 gtp
```

2. Configure GTP services for the P-GW interfaces called PGW1-MBG1 with path management disabled.

```
[edit unified-edge gateways pgw PGW1-MBG1 gtp]
user@pgw-sgw-1# set interface lo0.0
user@pgw-sgw-1# set interface v4-address 10.33.33.33
user@pgw-sgw-1# set n3-requests 5
user@pgw-sgw-1# set t3-response 3
user@pgw-sgw-1# set echo-interval 60
user@pgw-sgw-1# set path-management disable
user@pgw-sgw-1# set echo-n3-requests 5
user@pgw-sgw-1# set echo-t3-responses 30
```

3. Configure GTP services for the P-GW interfaces called PGW2-MBG1 with path management disabled.

```
[edit unified-edge gateways pgw PGW2-MBG1 gtp]
user@pgw-sgw-1# set interface lo0.0
user@pgw-sgw-1# set interface v4-address 10.44.44.44
user@pgw-sgw-1# set n3-requests 5
user@pgw-sgw-1# set t3-response 3
user@pgw-sgw-1# set echo-interval 60
user@pgw-sgw-1# set path-management disable
user@pgw-sgw-1# set echo-n3-requests 5
user@pgw-sgw-1# set echo-t3-responses 30
```

### Configuring GTP Services for the S-GW Named SGW1-MBG1 and SGW2-MBG1

**CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge gateways sgw SGW1-MBG1 gtp interface lo0.0
set unified-edge gateways sgw SGW1-MBG1 gtp interface v4-address 10.11.11.11
set unified-edge gateways sgw SGW1-MBG1 gtp path-management disable
set unified-edge gateways sgw SGW1-MBG1 gtp control path-management disable
set unified-edge gateways sgw SGW1-MBG1 gtp data path-management disable
set unified-edge gateways sgw SGW1-MBG1 gtp slu echo-interval 60
set unified-edge gateways sgw SGW1-MBG1 gtp s11 echo-n3-requests 5
set unified-edge gateways sgw SGW1-MBG1 gtp s11 echo-t3-response 30
set unified-edge gateways sgw SGW2-MBG1 gtp interface lo0.0
set unified-edge gateways sgw SGW2-MBG1 gtp interface v4-address 10.22.22.22
set unified-edge gateways sgw SGW2-MBG1 gtp control path-management disable
set unified-edge gateways sgw SGW2-MBG1 gtp data path-management disable
set unified-edge gateways sgw SGW2-MBG1 gtp slu echo-interval 60
set unified-edge gateways sgw SGW2-MBG1 gtp s11 echo-n3-requests 5
set unified-edge gateways sgw SGW2-MBG1 gtp s11 echo-t3-response 30
```

**Step-by-Step Procedure** To configure GTP services:

1. Configure the GTP services for the S-GW called SGW-MBG1.

```
[edit]
user@pgw-sgw-1# edit unified-edge gateways sgw SGW-MBG1 gtp
```

2. Configure GTP services for the S-GW GTP interfaces for SGW1-MBG1 with path management disabled.

```
[edit unified-edge gateways sgw SGW1-MBG1 gtp]
user@pgw-sgw-1# set interface lo0.0
user@pgw-sgw-1# set interface v4-address 10.11.11.11
user@pgw-sgw-1# set path-management disable
user@pgw-sgw-1# set control path-management disable
user@pgw-sgw-1# set data path-management disable
user@pgw-sgw-1# set slu echo-interval 60
user@pgw-sgw-1# set s11 echo-n3-requests 5
user@pgw-sgw-1# set s11 echo-t3-resposnes 60
```

3. Configure GTP services for the S-GW GTP interfaces for SGW2-MBG1 with path management disabled.

```
[edit unified-edge gateways sgw SGW2-MBG1 gtp]
user@pgw-sgw-1# set interface lo0.0
user@pgw-sgw-1# set interface v4-address 10.22.22.22
user@pgw-sgw-1# set path-management disable
user@pgw-sgw-1# set control path-management disable
user@pgw-sgw-1# set data path-management disable
user@pgw-sgw-1# set slu echo-interval 60
user@pgw-sgw-1# set s11 echo-n3-requests 5
user@pgw-sgw-1# set s11 echo-t3-resposnes 60
```

### Configure the APNs for the P-GW

- CLI Quick Configuration** To quickly configure this example, copy the following commands and paste them into the router terminal window:
- ```
[edit]
set unified-edge gateways ggsn-pgw PGW1-MBG1 apn-services apns APN1
set unified-edge gateways ggsn-pgw PGW1-MBG1 apn-services apns APN1 mobile interface
mif.3
set unified-edge gateways ggsn-pgw PGW1-MBG1 apn-services apns APN1
address-assignment local
set unified-edge gateways ggsn-pgw PGW1-MBG1 apn-services apns APN1 selection-mode
from-ms
set unified-edge gateways ggsn-pgw PGW2-MBG1 apn-services apns APN2
set unified-edge gateways ggsn-pgw PGW2-MBG1 apn-services apns APN1 mobile interface
mif.4
set unified-edge gateways ggsn-pgw PGW2-MBG1 apn-services apns APN1
address-assignment local
set unified-edge gateways ggsn-pgw PGW2-MBG1 apn-services apns APN1 selection-mode
from-ms
```
- Step-by-Step Procedure** To configure APNs for the P-GWs called PGW1-MBG1 and PGW2-MBG1:
1. Configure APN1 for the P-GW called PGW-MBG1.
 

```
[edit]
user@pgw-sgw-1# edit unified-edge gateways ggsn-pgw PGW1-MBG1 apn-services
apns APN1
[edit unified-edge gateways ggsn-pgw PGW1-MBG1 apn-services apns APN1]
user@pgw-sgw-1# set mobile-interface mif.3
user@pgw-sgw-1# set address-assignment local
user@pgw-sgw-1# set selection-mode from-ms
```
  2. Configure APN2 for the P-GW called PGW2-MBG1.
 

```
[edit]
user@pgw-sgw-1# edit unified-edge gateways ggsn-pgw PGW2-MBG1 apn-services
apns APN2
[edit unified-edge gateways ggsn-pgw PGW2-MBG1 apn-services apns APN2]
user@pgw-sgw-1# set mobile-interface mif.4
user@pgw-sgw-1# set address-assignment local
user@pgw-sgw-1# set selection-mode from-ms
```

## Verification

### Verifying Gateway Status

- Purpose** Verify the gateways for the broadband gateway.

**Action**    user@pgw-sgw-1> **show unified-edge gateways brief**

Total number of configured gateways: 4

Gateway name: PGW1-MBG1  
Gateway type: ggsn-pgw  
Gateway id: 1

Gateway name: PGW2-MBG1  
Gateway type: ggsn-pgw  
Gateway id: 2

Gateway name: SGW1-MBG1  
Gateway type: sgw  
Gateway id: 3

Gateway name: SGW2-MBG1  
Gateway type: sgw  
Gateway id: 4

**Meaning**    The **show unified-edge gateways brief** command displays information about the configured gateways.

**Related Documentation**

- [Example: Configuring a Collocated P-GW and S-GW on page 708](#)
- [Example: Configuring a Standalone S-GW on page 702](#)

## PART 12

# Index

- [Index on page 737](#)
- [Index of Statements and Commands on page 751](#)



# Index

## Symbols

#, comments in configuration statements.....	xxviii
( ), in syntax descriptions.....	xxviii
3G networks	
broadband gateway.....	25
GGSN.....	35
< >, in syntax descriptions.....	xxvii
[ ], in configuration statements.....	xxviii
{ }, in configuration statements.....	xxviii
(pipe), in syntax descriptions.....	xxviii

## A

AAA	
AAA profile configuration example.....	221
configuration example.....	213
configuration overview.....	167
configuration steps.....	199
configuring RADIUS servers.....	200
network element group configuration	
example.....	220
network elements.....	171
network elements configuration example.....	219
RADIUS configuration example.....	216
scalability and redundancy features.....	170
server failover.....	170
verifying the configuration.....	223
with Diameter base protocol.....	255
AAA profile.....	169
accounting options.....	205
applying to an APN.....	211
authentication options.....	205
configuration example.....	221
configuration steps.....	204
excluding or ignoring RADIUS attributes.....	207
overview.....	172
RADIUS options.....	173, 210
access point name.....	621
access point name delete .....	620
access point name modify.....	596
Access-Accept messages.....	179
Access-Request messages.....	174

accounting	
AAA profile options.....	173, 205
network element groups.....	172, 204
overview.....	168
Accounting On messages.....	195
Accounting Start messages.....	182
Accounting Stop messages.....	190
action profiles See PCC action profiles	
activate maintenance mode.....	598
address assignment	
APN configuration.....	122
by the AAA server.....	211, 212
configuring AAA server override.....	212
Advice of Charge	
overview.....	440
service filter configuration.....	495
service set and filter overview.....	441
aggregate maximum bit rate See AMBR	
allocation and retention priority See ARP	
AMBR	
configuring	
downlink.....	525, 533
uplink.....	525, 533
overview.....	504, 508
ams	
changing .....	614
AMS interface	
changing example.....	643
anchor interface DPCs and MPCs	
data path.....	10
anchor session DPCs	
data path.....	10
anchors	
broadband gateway.....	73, 84
configuring on broadband gateway.....	75
APN	
configuration example.....	143
HTTP header enrichment.....	153, 154, 157
network behind mobile.....	148, 150
APNs	
AAA configuration example.....	222
applying an AAA profile.....	211
broadband gateway.....	113, 133, 134
configuring address assignment.....	121, 122, 211
configuring charging profiles.....	131
configuring general APN parameters.....	117
configuring QoS local policy profiles.....	131
configuring service selection.....	135

configuring user options.....	141	brackets	
mobile network.....	32	angle, in syntax descriptions.....	xxvii
architecture		square, in configuration statements.....	xxviii
3G networks.....	25	broadband gateway	
ARP.....	505	3G networks.....	25
in 3G networks.....	504	address assignment configuration.....	122
in 4G networks.....	504	anchors.....	73, 84
overview.....	504	and GGSN.....	11
<i>See also</i> preemption		and IPv6 protocol.....	248
AuC		APN charging profiles configuration.....	131
mobile network.....	36	APN configuration.....	113, 117
authentication		APN configuration example.....	143
AAA profile options.....	172, 205	APN QoS local policy profiles	
overview.....	167	configuration.....	131
<b>B</b>		APN service selection configuration.....	135
background traffic class		APNs configuration.....	133, 134
description.....	501, 502	charging.....	429
bandwidth pools.....	506	chassis configuration.....	68
configuring.....	518	collocated P-GW and S-GW.....	17
APN level.....	506	configuring anchors .....	75
downlink.....	538	configuring call rate statistics.....	47
system level.....	506, 538	configuring charging.....	444
uplink.....	538	configuring fragment reassembly.....	98
<i>See also</i> overview		configuring gateways.....	45, 57
bearer binding		configuring HPLMNs.....	45, 57
overview.....	361	configuring idle-mode buffering.....	57
triggering bearer requests.....	362	configuring IP fragment reassembly.....	96, 99
bearer load		configuring local policies.....	46
configuring		configuring maximum bearers.....	57
in 3G/4G networks.....	520	configuring online charging.....	486
bearers		configuring preemption.....	57
configuring maximum number		configuring profiles.....	58
APN level.....	518	configuring QoS.....	581
system level.....	517	configuring S-GW global charging	
initial QoS level.....	500	profiles.....	446
managing load.....	507	control packet flow.....	5
maximum number, at system or APN		data path.....	10, 300
level.....	507	downlink payload packet flow.....	8
mobile network.....	33	functions.....	41
preempting.....	507	general gateway.....	49
rejecting based on		HTTP header enrichment.....	153, 154, 157
maximum traffic class.....	508	interface DPC or MPC configuration.....	72
upgrading based on		interface redundancy.....	80
AMBR.....	525, 533	interfaces redundancy configuration	
MBR.....	528, 529, 534, 535	example.....	86
binding		IP fragment reassembly overview.....	91
configuring Diameter.....	271	IP fragments.....	94
braces, in configuration statements.....	xxviii	IPv6 configuration example.....	250
		IPv6 protocol.....	247



- mobile interface configuration.....133, 134
- mobile options.....51
- network behind mobile.....146
- offline charging.....431
- online charging overview.....433
- P-GW.....11, 17, 19, 20
- physical interface overview.....69
- QoS configuration example.....542
- redundancy configuration.....78
- redundancy configuration example.....86
- restriction value configuration.....121
- Routing Engine redundancy.....78
- S-GW.....12, 17, 19, 20
- S-GW user packet flow.....16
- S1 interface.....39
- service and tracking areas.....40
- session DPC configuration.....70
- session DPC overview.....69
- session DPC redundancy.....79
- session DPC redundancy configuration
  - example.....86
- software reassemblyconfiguration
  - example.....107
- system architecture.....3
- traceoptions.....55, 59, 62, 338, 448, 451
- uplink payload packet flow.....7
- user options configuration.....141
- user-session routing.....115
- VRF configuration.....134
- Broadband Gateway
  - AAA configuration.....167
  - configuring
    - QoS, overview.....516
  - GGSN.....35
  - resource manager.....52
- C**
- CAC
  - bandwidth pools.....506
  - enforcing.....506
  - maximum bearers.....507
  - overview.....506
  - preemption, enabling.....519
  - resource thresholds.....507
- call admission control See CAC
- call rate statistics
  - configuring on broadband gateway.....47
  - monitoring.....48
- CDR profiles
  - configuring.....464
- CDRs
  - GTP Prime properties.....453
- Change of Authorization (CoA) Messages.....197
- charging
  - configuring.....443, 472
  - configuring on broadband gateway.....444, 486
  - configuring S-GW global profiles.....446
  - configuring S-GW selection order.....446
  - offline.....431
  - on broadband gateway.....429
  - online.....433
  - S-GW local persistent storage
    - traceoptions.....451
  - S-GW traceoptions.....448
- charging configurations
  - managing.....484
  - monitoring.....484
- charging control
  - overview.....352
- charging profiles
  - APN
    - configuring.....469
  - APN configuration.....131
  - CDR profiles.....464
  - changing.....601
  - configuring.....467
  - deleting.....605
  - modifying.....601
  - transport profiles.....459
  - trigger profiles.....462
- chassis
  - broadband gateway.....68
  - monitoring.....76
  - redundancy configuration.....80, 82
- classifier profiles
  - configuring
    - for 3G and 4G networks.....521
- collocated
  - P-GW configuration.....708
  - S-GW configuration.....708
- collocated gateways
  - P-GW and S-GW.....19, 20
- comments, in configuration statements.....xxviii
- configuration
  - broadband gateway.....68
  - broadband gateway interface PFEs.....78
  - broadband gateway services PICs.....78

configuration example		configuring restriction value	
APN.....	143	APN configuration.....	121
for QoS.....	542	configuring S-GW	
IPv6.....	250	charging configuration.....	444, 446
redundancy.....	86	gateways configuration.....	57
software reassembly.....	107	profile configuration.....	58
configuring		QoS configuration.....	581
GTP parameters.....	325, 335, 337	configuring service selection	
S1-U interface.....	332	APNs.....	135
S11 interface.....	328	configuring session DPC	
S12 interface.....	330	control messages.....	70
S4 interface.....	333	redundancy.....	80
configuring address assignment		configuring session DPCs	
APN configuration.....	122	anchor configuration.....	75
configuring APNs		configuring user options	
gateways configuration.....	45	APN configuration.....	141
configuring broadband gateway		connection set identifiers.....	298
APN configuration.....	113, 117	control messages	
configuring call rate statistics		session DPC configuration.....	70
gateways configuration.....	47	control packet flow	
configuring charging profiles		broadband gateway.....	5
APNs.....	131	control plane	
configuring chassis		configuring GTP services	
interfaces for mobility redundancy.....	82	for GGSN/P-GW.....	306
session DPC redundancy.....	80	conventions	
configuring HPLMNs		text and syntax.....	xxvii
gateways.....	45, 57	conversational traffic class	
configuring idle-mode buffering		description.....	501, 502
gateways.....	57	CoS policy profile	
configuring interface DPCs or MPCs		AMBR in.....	508
user traffic.....	72	configuring	
configuring interfaces for mobility		in 3G networks.....	526
redundancy.....	82	in 3G/4G networks.....	531
configuring local policies		in 4G networks.....	523
gateways.....	46	GBR in.....	509
configuring maximum bearers		maximum QCI in.....	508
gateways.....	57	maximum traffic class in.....	508
configuring mobile interfaces		MBR in.....	508
mobility.....	133, 134	overview.....	508
configuring PFEs		policer actions.....	509
anchor configuration.....	75	CPU	
configuring preemption		managing load .....	507
gateways.....	57	CPU load	
configuring QoS local policy profiles		configuring	
APNs.....	131	in 3G/4G networks.....	520
configuring redundancy		curly braces, in configuration statements.....	xxviii
interfaces for mobility.....	82	customer support.....	xxviii
session DPC.....	80	contacting JTAC.....	xxviii

**D**

data path	
broadband gateway.....	10, 300
traceoptions.....	55, 62
data plane	
configuring GTP services	
for GGSN/P-GW.....	308
dead server detection.....	171
configuring.....	202
default settings	
preemption.....	516
resource thresholds .....	507, 508
delete access point name.....	599
deployment	
mobile network.....	36
DHCP	
AAA address override.....	212
configuring	
APN.....	245
overview.....	235
DHCP proxy client	
configuring.....	242
DHCP proxy clients	
understanding.....	236
DHCPv4 proxy client profiles	
configuring.....	237
DHCPv6 proxy client profiles	
configuring.....	240
Diameter applications	
Diameter AVPs, configuring.....	267, 269
parameter configuration.....	264
Diameter AVPs	
for Gx applications, configuring.....	269
for Gy applications, configuring.....	267
Diameter base protocol.....	255
binding configuration.....	271
event logging.....	264
flags for tracing operations.....	265
log filenames for tracing operations.....	265
network element configuration.....	263
origin attribute configuration.....	260
peer configuration.....	261
peers for tracing operations.....	266
tracing operations.....	264
transport configuration.....	260
Diameter profiles	
configuring.....	266
Diameter AVPs, configuring.....	267, 269
overview.....	256

diffserv model	
QoS support on broadband gateway.....	500
Disconnect Request messages.....	196
documentation	
comments on.....	xxviii
downlink payload packet flow	
broadband gateway.....	8
DPCs	
configuring interface DPCs.....	72
DSCP marking	
subscriber packets.....	540, 541
dynamic policies See policy and charging	
enforcement function	
Diameter AVPs, configuring.....	269
overview.....	359
provisioning	
pull mode.....	360
push mode.....	360
dynamic requests.....	169
enabling for a RADIUS server.....	201

**E**

egress rewrite rules	
configuring.....	539
overview	
overview.....	510
EIR	
mobile network.....	36
EPC	
mobile network.....	30
errors	
data path.....	300
event trigger reporting	
understanding.....	363
event triggers	
configurable triggers.....	363
configuring.....	373
implicit.....	363
overview.....	363
evolved packet core	
mobile network.....	30
example	
changing AMS interface.....	643
changing charging profile.....	622
changing transport profile.....	624
collocated P-GW configuration.....	708
collocated S-GW configuration.....	708
deleting services PIC.....	640
deleting session PIC.....	636

Diameter configuration.....	271, 279
GTP configuration.....	340
HTTP header enrichment.....	157
multigateway P-GW configuration.....	719
multigateway S-GW configuration.....	719
network behind mobile.....	150
S-GW configuration.....	702
S-GW QoS and CAC configuration.....	582
examples	
configuring IP fragment reassembly on	
broadband gateway.....	96, 99
configuring online charging.....	486
exceed-action policer	
overview.....	510
exit maintenance mode.....	599
<b>F</b>	
failover	
broadband gateway anchors.....	84
flow identifiers <i>See</i> service data flow filters	
font conventions.....	xxvii
fragment	
broadband gateway handling.....	94
fragment reassembly	
configuring on broadband	
gateway.....	96, 98, 99
on broadband gateway.....	91
functions	
S-GW.....	41
functions in mobile network	
APNs.....	32
packet data network gateway.....	28
<b>G</b>	
gateway	
changing parameters.....	617
gateway configurations	
monitoring.....	48
gateways	
configuring on broadband gateway.....	45, 57
gating control	
overview.....	352
GBR	
overview.....	501, 509
GBR bearers.....	506
behavior.....	353
<i>See also</i> bandwidth pools	
general gateway	
traceoptions.....	49
GGSN	
broadband gateway.....	11, 35
functions in mobile network.....	23, 26
in 3G networks.....	35
Gn interface	
configuring GTP services	
for GGSN/P-GW.....	312
Gp interface	
configuring GTP services	
for GGSN/P-GW.....	314
GPRS Tunneling Protocol.....	595
GTP	
configuring.....	325, 335, 337
connection set identifiers.....	298
echo requests	
version support for.....	291
example.....	340
GPRS interfaces.....	288
overview.....	289
path management .....	290
default settings.....	290
disabling.....	323
echo requests.....	291
echo-request messages.....	291
overview.....	290
path failure.....	292
path success.....	291
restart counters.....	297
supported versions.....	287
traceoptions.....	338
tunnel endpoint identifiers.....	299
tunnel management	
create requests.....	295
default settings.....	294
overview.....	294
path failure.....	296
path success.....	295
request messages.....	295
update/delete requests.....	295, 296
version support.....	294
tunnel management functions.....	294
GTP interface address change.....	593
GTP interface delete.....	595
GTP Prime peers	
GTP Prime properties.....	454
GTP Prime properties	
configuring.....	453, 454
GTP redirect <i>See</i> user-session routing	

- GTP services
  - configuring
    - 3GPP interfaces in different VRFs.....318
    - control plane for GGSN/P-GW.....306
    - data plane for GGSN/P-GW.....308
    - default settings.....303
    - GGSN.....320
    - GGSN/P-GW.....305
    - Gn interface.....312
    - Gp interface.....314
    - loopback address.....304
    - peer group.....321
    - S5 and S8 interfaces.....315, 317
    - S5 interface.....309
    - S8 interface.....310
    - trace options.....323
  - configuring on gateway
    - overview.....302
- GTP-C messages
  - route lookup.....299
- GTP-U errors
  - data path.....300
- guaranteed bit rate See GBR
- Gx interface
  - provisioning of rules
    - overview.....359
- H**
  - home users
    - mobile network.....12
  - HSS
    - mobile network.....36
  - HTTP header enrichment
    - APN.....153, 154, 157
    - example.....157
    - P-GW.....153, 154
- I**
  - icons defined, notice.....xxvi
  - information element (IE)
    - initial QoS level.....500
  - ingress rewrite rules
    - configuring.....539
    - overview
      - overview.....510
  - interactive traffic class
    - description.....501, 502
  - interface DPC and MPC
    - anchors.....73
    - interface DPCs or MPCs
      - configuring for user traffic.....72
    - interface mobile interfaces
      - configuring.....133, 134
    - interface redundancy configuration example
      - broadband gateway.....86
    - interfaces
      - GTP.....325, 335, 337, 340
      - mobile
        - applying rewrite rules.....540, 541
      - S1-U.....332
      - S11.....328
      - S12.....330
      - S4.....333
    - interfaces for mobility
      - redundancy configuration.....82
    - Interim-Update messages.....186
    - IP fragment reassembly
      - configuring on broadband gateway.....96, 99
      - on broadband gateway.....91
    - IP fragments
      - broadband gateway handling.....94
    - IPv6
      - configuration example.....250
      - mobile network.....38
    - IPv6 protocols
      - broadband gateway parameters.....247, 248
- L**
  - local persistent storage
    - S-GW traceoptions.....451
  - local policies
    - configuring on broadband gateway.....46
    - specifying
      - bandwidth pools.....538
      - classifier profiles.....537
      - policy profiles.....537
      - resource thresholds.....537
  - local policies profile
    - configuring.....537
  - local policy
    - applying
      - system level.....538
  - log files
    - configuring Diameter base protocol trace.....264
  - loopback address
    - configuring for GTP services.....304
  - LTE See networks

**M**

maintenance mode.....	592
changing AMS example.....	643
changing ams parameters.....	614
changing gateway parameters.....	617
deleting services PIC .....	612
deleting services PIC example.....	640
deleting session PIC .....	610
deleting session PIC example.....	636
manuals	
comments on.....	xxviii
maximum bearers	
configuring	
APN level.....	518
system level.....	517
maximum bit rate See MBR	
maximum pending requests.....	171
maximum QCI	
overview.....	508
maximum traffic class	
overview.....	508
MBR	
configuring	
downlink.....	528, 529, 534, 535
uplink.....	528, 529, 534, 535
configuring in traffic classes.....	537
overview.....	501, 508
memory	
managing load .....	507
memory load	
configuring	
in 3G/4G networks.....	521
mobile address pool change.....	607
mobile address pool delete.....	609
mobile charging	
flags for tracing operations.....	471
log filenames for tracing operations.....	471
tracing operations.....	470
mobile interface	
applying rewrite rules.....	510
mobile interface change.....	633
mobile interfaces	
applying egress rewrite rules.....	541
applying ingress rewrite rules.....	540
configuring .....	133, 134
mobile network	
3G.....	23
4G/LTE.....	23
APNs.....	32

bearers.....	33
broadband gateway architecture.....	3
deployment.....	36
EPC.....	30
functions.....	41
GGSN.....	23, 26
IPv6.....	38
network behind mobile.....	146
P-GW.....	19, 20, 23, 26, 38
packet data network gateway.....	28
S-GW.....	12, 19, 20
S-GW user packet flow.....	16
S1 interface.....	39
service and tracking areas.....	40
user types.....	12
mobile options	
traceoptions.....	51
mobile pool groups	
configuring.....	230
overview.....	229
mobile pools	
configuring.....	230
overview.....	229
mobile subscribers	
CDR profiles.....	464
charging profiles.....	467
APN.....	469
monitoring.....	484
persistent storage of CDR.....	455
tracing operations.....	470
transport profiles.....	459
trigger profiles.....	462
mobility address pool delete.....	631
mobility pool change.....	626
monitoring	
chassis configuration.....	76
MPCs	
configuring interface MPCs.....	72
multigateway	
P-GW configuration.....	719
S-GW configuration.....	719

**N**

network behind mobile	
APN.....	148, 150
P-GW.....	146, 148, 150
network element.....	170
configuring Diameter.....	263

network element group	
configuration example.....	220
specifying for accounting.....	205
network element groups	
configuring.....	204
overview.....	172
network elements	
configuration example.....	219
configuring.....	203
dead server detection.....	171, 202
load-balancing algorithm.....	171
maximum pending requests.....	171
overview.....	171
server priority.....	171
specifying for accounting.....	205
specifying for authentication.....	205
networks	
3G	
ARP.....	500
classifying subscriber traffic.....	500
GBR.....	500
MBR.....	500
QoS parameters.....	500
4G	
AMBR.....	503
ARP.....	503
classifying subscriber traffic.....	503
QoS parameters.....	503
non-GBR bearers	
behavior.....	353
notice icons defined.....	xxvi
<b>O</b>	
offline charging	
configuring.....	443
online charging	
configuring.....	472
configuring on broadband gateway.....	486
Diameter AVPs, configuring.....	267
on broadband gateway.....	433
origin attributes	
configuring Diameter endpoint.....	260
overview	
interface redundancy.....	80
physical interface types.....	69
Routing Engine redundancy.....	78
session DPC.....	69
session DPC redundancy.....	79

## P

P-GW	
broadband gateway.....	11
collocated example.....	708
collocated with S-GW.....	19, 20, 708
function in mobile network.....	26
functions in mobile network.....	23
HTTP header enrichment.....	153, 154
multigateway example.....	719
multigateway with S-GW.....	719
network behind mobile.....	146, 148, 150
packet data network gateway	
functions in mobile network.....	28
packet flow	
broadband gateway control.....	5
packet flow downlink	
broadband gateway payload.....	8
packet flow uplink	
broadband gateway payload.....	7
parentheses, in syntax descriptions.....	xxviii
path management See GTP	
payload flow downlink	
broadband gateway downlink.....	8
payload flow uplink	
broadband gateway uplink.....	7
PCC action profiles	
configuring.....	369
PCC rulebase	
configuring.....	372
PCC rules	
action profiles	
configuring.....	369
configuring.....	370, 371
dynamic policies	
overview.....	359
static policies	
overview.....	361
PCEF operations	
troubleshooting.....	378
PCEF profile for dynamic policies	
Diameter AVPs, configuring.....	269
PCEF profile for dynamic services	
applying to an APN.....	389, 417
PCEF profile for static services	
applying to an APN.....	389, 417
PCI flags.....	505
PCRF	
mobile network.....	36

PDP contexts		
bearers.....	33	
GBR.....	501	
initial QoS level.....	500	
MBR.....	501	
peer		
configuring Diameter.....	261	
peer group		
configuring GTP services.....	321	
persistent storage		
configuring.....	455	
configuring the SSD.....	457, 458	
ejecting the SSD.....	458	
initializing the SSD.....	457	
tracing operations.....	456	
physical interfaces		
broadband gateway.....	69	
PLMN		
mobile network.....	36	
PLMNs		
configuring on broadband gateway.....	45	
mobile network.....	12	
policer action		
configuring		
overview.....	509	
policer configuration		
exceed-action.....	510	
overview.....	509	
violate-action.....	509, 510	
policies		
configuring on broadband gateway.....	46	
policing, subscriber traffic.....	353	
Policy and Charging Control		
overview.....	351, 353	
rules		
dynamic policies.....	352, 354	
provisioning.....	359	
static policies.....	352	
policy and charging control rules		
application-aware services.....	365	
policy and charging enforcement function		
configuration		
overview.....	348	
configuration example.....	379, 397	
dynamic policies		
configuring.....	375	
event triggers		
configuring.....	373	
flow identifiers		
configuring.....	367	
Layer 7 rules		
static policies.....	355	
operations		
troubleshooting.....	378	
overview.....	347	
PCC rulebase		
configuring.....	372	
PCC rules		
configuring.....	370, 371	
PCEF profile		
applying to an APN.....	389, 417	
PCEF profile for dynamic policies		
configuring.....	375	
PCEF profile for static policies		
configuring.....	377	
service data flow filters		
configuring.....	367	
static policies		
configuring.....	377	
predefined static policies		
overview.....	361	
preemption		
capability.....	505	
enabling.....	519	
enabling.....	519	
overview.....	505	
PCI flags.....	505	
PVI flags.....	505	
vulnerability.....	505, 519	
profiles		
configuring on broadband gateway.....	58	
PVI flags.....	505	
<b>Q</b>		
QCI		
overview.....	503	
QoS		
class identifiers.....	503	
configuration example.....	542	
configuring		
local policies.....	537	
configuring on Broadband Gateway		
overview.....	516	
configuring on broadband gateway.....	581	
Differentiated Services model.....	500	
initial level assigned to bearer.....	500	



- local policy
  - applying at apn level.....538
  - applying at system level.....538
  - monitoring.....579
  - NQN flags and upgrade behavior.....513
  - overview.....499
  - traffic classes.....500
  - upgrade flags and upgrade behavior.....513
- QoS and CAC
  - S-GW configuration.....582
- QoS Class Identifier See QCI
- QoS classifier profiles
  - configuring
    - 3G/4G networks.....521
- QoS local policy profiles
  - APN configuration.....131
- QoS profiles
  - configuring
    - classifier profile.....521
    - CoS policy profile.....531
    - CoS policy profile, in 3G
      - networks.....523, 526
    - local policy.....537
    - resource threshold profile.....520
- Quality of service See QoS
- quality of service (QoS) control
  - overview.....352
- R**
- RADIUS attributes.....173
  - excluding or ignoring in RADIUS
    - messages.....207
  - supported in Access-Accept messages.....179
  - supported in Access-Requests.....174
  - supported in Accounting On messages.....195
  - supported in Accounting Start messages.....182
  - supported in Accounting Stop messages.....190
  - supported in CoA messages.....197
  - supported in Disconnect Request
    - messages.....196
  - supported in Interim-Update messages.....186
- RADIUS options.....173
  - specifying in AAA profile.....210
- RADIUS servers
  - assigning to network elements.....203
  - configuration example.....216
  - configuring.....200
  - enabling dynamic requests.....201
- redundancy
  - anchor failover.....84
  - broadband gateway.....78, 79, 80
  - configuration example.....86
  - configuring session DPC.....80, 82
- redundancy configuration example
  - broadband gateway.....86
- rejecting
  - maximum active bearers.....517
- resource management
  - traceoptions.....52
- resource threshold profiles
  - configuring
    - in 3G/4G networks.....520
- resource thresholds
  - default settings.....507
  - managing load
    - bearer.....507
    - CPU.....507
    - memory.....507
  - overview .....507
  - preempting bearers.....507
- restart counters.....297
- restriction value
  - APN configuration.....121
- rewrite rules
  - default DSCP marking
    - .....540, 541
  - egress
    - applying to mobile interfaces.....541
    - configuring.....539
    - overview.....510
  - ingress
    - applying to mobile interfaces.....540
    - configuring.....539
    - overview.....510
  - overview.....510
- roaming users
  - mobile network.....12
- route lookup
  - GTP-C messages.....299
- router advertisement
  - IPv6 and broadband gateway.....247, 248
- router solicitation
  - IPv6 and broadband gateway.....247, 248

## S

## S-GW

charging traceoptions.....	448
collocated example.....	708
collocated with P-GW.....	19, 20, 708
configuring global charging profiles.....	446
example.....	582, 702
functions.....	41
GTP.....	325, 335, 337, 340
GTP traceoptions.....	338
in mobile network.....	12
local persistent storage traceoptions.....	451
multigateway example.....	719
multigateway with P-GW.....	719
QoS and CAC.....	582
S1 interface.....	39
S1-U interface.....	332
S11 interface.....	328
S12 interface.....	330
S4 interface.....	333
service and tracking areas.....	40
standalone.....	702
traceoptions.....	59
user packet flow.....	16
S1 interface	
S-GW.....	39
S1-U	
configuring.....	332
S11	
configuring.....	328
S12	
configuring.....	330
S4	
configuring.....	333
s5 interface	
configuring GTP services	
for GGSN/P-GW.....	309
s8 interface	
configuring GTP services	
for GGSN/P-GW.....	310
selection order	
S-GW charging configuration.....	446
service areas	
S-GW.....	40
service data flow filters	
configuring.....	367
overview.....	349

service filters	
Advice of Charge.....	441
Advice of Charge configuration.....	495
service selection	
APN configuration.....	135
service sets	
Advice of Charge.....	441
services	
application-aware policy and charging control	
rules.....	365
services PIC	
deleting .....	612
deleting example.....	640
session DPC	
anchors.....	73
broadband gateway.....	69
configuring.....	70
redundancy configuration.....	80
session DPC redundancy configuration example	
broadband gateway.....	86
session PIC	
deleting .....	610
deleting example.....	636
software reassembly	
configuration example.....	107
standalone	
S-GW configuration.....	702
static Gx policy	
overview.....	359
static Gx rules See Policy and Charging Control,	
dynamic policies	
static policies See policy and charging enforcement	
function See Policy and Charging Control	
streaming traffic class	
description.....	501, 502
subscriber packets	
DSCP marking on.....	540, 541
subscriber traffic	
policing.....	509
support, technical See technical support	
syntax conventions.....	xxvii
system architecture	
broadband gateway.....	3

## T

technical support	
contacting JTAC.....	xxviii
TEID See tunnel endpoint identifiers	

Top-Up	
Advice of Charge.....	440
trace options	
configuring for GTP.....	323
traceoptions	
charging.....	448
data path.....	55, 62
general gateway.....	49
GTP.....	338
local persistent storage.....	451
mobile options.....	51
resource manager.....	52
S-GW.....	59
tracing operations	
Diameter base protocol.....	264
for persistent storage.....	456
mobile charging.....	470
mobile subscribers.....	470
tracking areas	
S-GW.....	40
traffic classes	
overview.....	500
transport	
configuring Diameter.....	260
transport profiles	
changing.....	603
configuring	
offline charging.....	459
online.....	473
deleting.....	606
modifying.....	603
trigger profiles	
configuring.....	462
online charging.....	476
tunnel endpoint identifiers.....	299
route lookup.....	299
tunnel management See GTP	
 <b>U</b>	
UMTS See networks	
uplink payload packet flow	
broadband gateway.....	7
user options	
APN configuration.....	141
user types	
mobile network.....	12
user-session routing	
broadband gateway.....	115
 <b>V</b>	
violate-action policer	
overview.....	509, 510
visiting users	
mobile network.....	12
VRFs	
broadband gateway.....	134
VSA	
excluding from RADIUS messages.....	207
supported.....	169
 <b>W</b>	
wait-accounting statement	
configuring.....	212



# Index of Statements and Commands

## B

bearer binding	
overview.....	361
triggering bearer requests.....	362
broadband gateway	
interface redundancy.....	80
interfaces redundancy configuration	
example.....	86
redundancy configuration.....	78
redundancy configuration example.....	86
Routing Engine redundancy.....	78
session DPC redundancy.....	79
session DPC redundancy configuration	
example.....	86

## C

charging control	
overview.....	352
chassis	
redundancy configuration.....	80, 82
configuration	
broadband gateway interface PFEs.....	78
broadband gateway services PICs.....	78
configuration example	
redundancy.....	86
configuring chassis	
interfaces for mobility redundancy.....	82
session DPC redundancy.....	80
configuring interfaces for mobility	
redundancy.....	82
configuring redundancy	
interfaces for mobility.....	82
session DPC.....	80
configuring session DPC	
redundancy.....	80

## D

DHCP	
configuring	
APN.....	245
DHCP proxy client	
configuring.....	242
dynamic policies	
overview.....	359
provisioning	
pull mode.....	360
push mode.....	360

## E

event trigger reporting	
understanding.....	363
event triggers	
configurable triggers.....	363
implicit.....	363
overview.....	363

## F

flow identifiers See service data flow filters

## G

gating control	
overview.....	352
GBR bearers	
behavior.....	353
Gx interface	
provisioning of rules	
overview.....	359

## I

interface redundancy configuration example	
broadband gateway.....	86
interfaces for mobility	
redundancy configuration.....	82

## N

non-GBR bearers	
behavior.....	353

## O

overview	
interface redundancy.....	80
Routing Engine redundancy.....	78
session DPC redundancy.....	79

**P**

## PCC rules

## dynamic policies

overview.....359

## static policies

overview.....361

policing, subscriber traffic.....353

## Policy and Charging Control

overview.....351, 353

## rules

provisioning.....359

## policy and charging enforcement function

## configuration

overview.....348

overview.....347

## predefined static policies

overview.....361

**Q**

## quality of service (QoS) control

overview.....352

**R**

## redundancy

broadband gateway.....78, 79, 80

configuration example.....86

configuring session DPC.....80, 82

## redundancy configuration example

broadband gateway.....86

**S**

## service data flow filters

overview.....349

## session DPC

redundancy configuration.....80

## session DPC redundancy configuration example

broadband gateway.....86

## static Gx policy

overview.....359