

MobileNext Broadband Gateway Configuration Guide

Release

11.2



Published: 2011-12-27

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
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
December 2011—R2 11.2

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	xxxv
Part 1	Overview	
Chapter 1	System Architecture	3
Chapter 2	Network Architecture	37
Part 2	System Configuration	
Chapter 3	Configuring Mobility on MX 3D Devices	61
Chapter 4	Configuring Redundancy on MX 3D Devices	73
Chapter 5	Configuring Mobile Edge Exception Handling	87
Part 3	APN Configuration	
Chapter 6	Configuring APNs	105
Part 4	Authorization and Addressing Configuration	
Chapter 7	Configuring AAA	147
Chapter 8	Configuring DHCP	207
Part 5	GPRS Tunneling Protocol (GTP) Configuration	
Chapter 9	Configuring GTP	213
Part 6	Charging Configuration	
Chapter 10	Charging Overview	271
Chapter 11	Configuring Charging	279
Part 7	Quality of Service Configuration	
Chapter 12	Configuring Quality of Service	309
Part 8	Maintenance	
Chapter 13	Maintenance Mode	393
Part 9	Monitoring and Troubleshooting	
Chapter 14	Monitoring	429
Chapter 15	Troubleshooting	457

Part 10	Examples	
Chapter 16	Example Configurations	471
Part 11	Complete Configuration Statement Hierarchy and Summary of Statements	
Chapter 17	Configuration Statement Hierarchy	553
Chapter 18	AAA on the Broadband Gateway	585
Chapter 19	Address Assignment and DHCP Configuration Statements	617
Chapter 20	Anchor Packet Forwarding Engine Redundancy and Aggregated Multiservices High Availability Configuration Statements	645
Chapter 21	APN Configuration Statements	677
Chapter 22	Charging Configuration Statements	769
Chapter 23	Class of Service (CoS) Configuration Statements	855
Chapter 24	Exception Handling Configuration Statements	897
Chapter 25	Gateway Maintenance Mode Configuration Statement	915
Chapter 26	GTP Configuration Statements	917
Chapter 27	Service Applications Configuration Statements	971
Chapter 28	System Architecture and Gateway Traceoptions Configuration Statements	981
Part 12	Command Reference	
Chapter 29	AAA Operational Commands	1017
Chapter 30	Anchor Packet Forwarding Engine Redundancy and Aggregated Multiservices High Availability Operational Commands	1053
Chapter 31	APN and Related Operational Commands	1071
Chapter 32	Charging Operational Commands	1109
Chapter 33	Class of Service (CoS) Operational Commands	1173
Chapter 34	Exception Handling Operational Commands	1183
Chapter 35	GPRS Tunneling Protocol (GTP) Operational Commands	1193
Chapter 36	Service Applications Operational Commands	1237
Chapter 37	System Architecture Operational Commands	1269
Part 13	Index	
	Index	1315
	Index of Statements and Commands	1337

Table of Contents

	About This Guide	xxxv
	Junos Documentation and Release Notes	xxxv
	Objectives	xxxvi
	Audience	xxxvi
	Supported Platforms	xxxvi
	Using the Indexes	xxxvii
	Using the Examples in This Manual	xxxvii
	Merging a Full Example	xxxvii
	Merging a Snippet	xxxviii
	Documentation Conventions	xxxviii
	Documentation Feedback	xl
	Requesting Technical Support	xl
	Self-Help Online Tools and Resources	xli
	Opening a Case with JTAC	xli
Part 1	Overview	
Chapter 1	System Architecture	3
	Overview of Broadband Gateway System Architecture	4
	Overview of Broadband Gateway System Control Packet Flow	6
	Overview of Broadband Gateway Uplink Payload Packet Flow	7
	Overview of Broadband Gateway Downlink Payload Packet Flow	9
	Overview of Broadband Gateway as GGSN or P-GW	10
	Understanding Mobile User Types	11
	Configuring Broadband Gateway Home PLMNs and Gateways	11
	Configuring Broadband Gateway Local Policies Application	12
	Configuring Broadband Gateway Call Rate Statistics	13
	Verifying the Gateway Configuration	14
	Configuring General Gateway Trace Options	15
	Configuring Mobile Options Trace Options	17
	Configuring Resource Manager Trace Options	19
	Serving Gateways and the MobileNext Broadband Gateway Overview	21
	Overview of Standalone S-GW User Plane Packet Flow	25
	MobileNext Broadband Gateway Configuration Overview	26
	Overview of Collocated Gateways: Control Plane	28
	Overview of Collocated Gateways: User Plane	29
	Configuring an S-GW on a Broadband Gateway	30
	Configuring S-GW-Specific Profiles	32
	Configuring S-GW Traceoptions	33

Chapter 2	Network Architecture	37
	Overview of Mobile Networks	37
	Overview of 3G Mobile Networks and the MobileNext Broadband Gateway	39
	Overview of GGSN and P-GW	40
	Overview of Packet Data Network Gateway Functions	42
	Overview of the Evolved Packet Core	44
	Overview of APNs	46
	Overview of PDP Contexts and Bearers	47
	Overview of GGSN and Broadband Gateway Deployment	49
	Overview of 4G/LTE and Broadband Gateway Deployment	50
	Overview of IPv6 and the Broadband Gateway	52
	Serving Gateway and the S1 Interface Overview	53
	Service Areas and Tracking Areas Overview	54
	Serving Gateway Functions Overview	55
Part 2	System Configuration	
Chapter 3	Configuring Mobility on MX 3D Devices	61
	MobileNext Broadband Gateway Chassis Overview	62
	Session DPCs for Mobility	63
	Overview of Mobility Interface Types	63
	Configuring Session DPCs for Mobility	64
	Configuring Interface DPCs or MPCs for User Mobility Traffic	66
	Example: Configuring the MobileNext Broadband Gateway Chassis	67
	Understanding the MobileNext Broadband Gateway Anchors	69
	Configuring Anchor Session DPCs and PFES	71
	Verifying the MobileNext Broadband Gateway Chassis Configuration	72
Chapter 4	Configuring Redundancy on MX 3D Devices	73
	Broadband Gateway Redundancy Overview	74
	Routing Engine Redundancy	74
	Session DPC Redundancy	75
	Interface Redundancy	76
	Configuring Session DPC Redundancy	76
	Configuring Interface Redundancy	78
	Understanding the Broadband Gateway Anchor Failover Behavior	80
	Example: Configuring Broadband Gateway Redundancy	82
Chapter 5	Configuring Mobile Edge Exception Handling	87
	Understanding the Broadband Gateway Exception Handling	88
	Understanding GTP-U Error Exception Handling	89
	Understanding Broadband Gateway IP Fragment Handling	90
	Configuring Fragment Reassembly Parameters	90
	Understanding IPv6 Protocol Parameters	92
	Configuring IPv6 Protocol Parameters	93
	Configuring Exception Handling Traceoptions	95
	Configuring S-GW Data Path Traceoptions	97
	Example: Configuring Broadband Gateway Exception Handling Parameters	99

Part 3	APN Configuration	
Chapter 6	Configuring APNs	105
	Configuring APNs on the MobileNext Broadband Gateway Overview	105
	General APN Parameters	106
	Restriction Value	106
	Anonymous Users	107
	Address Assignment	107
	Anchor DPC or MPC Failure Behavior	107
	Charging Profiles	107
	User-Session Routing Overview	107
	Configuring General APN Parameters on the Broadband Gateway	109
	Configuring the APN Name, Interface, and Type	109
	Configuring Servers for an APN	110
	Configuring APN Timers	111
	Configuring Miscellaneous APN Parameters	111
	Configuring the Restriction Value on a Broadband Gateway APN	113
	Configuring Anonymous Users on a Broadband Gateway APN	114
	Configuring Address Assignment on a Broadband Gateway APN	115
	Configuring Charging and Local Policy Profiles on a Broadband Gateway APN	119
	Configuring Mobile Interfaces for APNs	120
	Configuring Mobile Interface to APN Associations in VRFs	122
	Configuring APN Service Selection on a Broadband Gateway	123
	Example: Configuring Broadband Gateway APNs	126
	Networks Behind the Mobile Device Overview	130
	Configuring the Networks Behind the Mobile Equipment Feature	131
	Example: Configuring the Networks Behind the Mobile Device Feature	133
	HTTP Header Enrichment Overview	134
	Configuring HTTP Header Enrichment	135
	Example: Configuring HTTP Header Enrichment	138
Part 4	Authorization and Addressing Configuration	
Chapter 7	Configuring AAA	147
	Overview of AAA on the Broadband Gateway	148
	Authentication	148
	Accounting	149
	APN-Specific AAA Settings	149
	RADIUS-Initiated Dynamic Requests	150
	Support for RADIUS Attributes, Juniper Networks VSAs, and 3GPP VSAs	150
	Scalability and Redundancy	150
	Scalability	150
	Redundancy	151
	Network Elements	151
	Load Balancing Within Network Elements	151
	Server Priority	152
	Dead Server Detection	152
	Maximum Pending Requests for a Network Element	152

Network Element Groups	152
AAA Profiles	153
Authentication Options	153
Accounting Options	153
RADIUS Attributes to Ignore or Exclude	154
RADIUS Options	154
Supported Attributes in Access-Request Messages	155
RADIUS IETF Attributes Supported in Access-Request Messages	155
3GPP VSAs Supported in Access-Request Messages	157
Supported Attributes in Access-Accept Messages	159
RADIUS IETF Attributes Supported in Access-Accept Messages	160
3GPP VSAs Supported in Access-Accept Messages	161
Juniper Networks VSAs Supported in Access-Accept Messages	162
Supported Attributes in Accounting Start Messages	162
RADIUS IETF Attributes Supported in Accounting Start Messages	162
3GPP VSAs Supported in Accounting Start Messages	164
Supported Attributes in Accounting Interim Update Messages	166
RADIUS IETF Attributes Supported in Interim-Update Messages	166
3GPP VSAs Supported in Interim-Update Messages	168
Supported Attributes in Accounting Stop Messages	171
RADIUS IETF Attributes Supported in Accounting Stop Messages	171
3GPP VSAs Supported in Accounting Stop Messages	173
Supported Attributes in Accounting On Messages	175
RADIUS IETF Attributes Supported in Accounting On Messages	175
Supported Attributes in Disconnect Request Messages	176
RADIUS IETF Attributes Supported in Disconnect Request Messages	176
3GPP VSAs Supported in Disconnect Request Messages	177
Supported Attributes in Change of Authorization (CoA) Messages	177
RADIUS IETF Attributes Supported in CoA Messages	177
3GPP VSAs Supported in CoA Messages	178
Configuring AAA on the Broadband Gateway	179
Configuring Interaction Between the Broadband Gateway and RADIUS Servers	179
Configuring RADIUS-Initiated Dynamic Request Support	181
Configuring Dead Server Detection	181
Configuring Network Elements	182
Configuring Network Element Groups	183
Configuring an AAA Profile	184
Configuring Authentication Settings in an AAA Profile	184
Configuring Accounting Settings in an AAA Profile	185
Configuring RADIUS Attribute Usage for an AAA Profile	186
Specifying RADIUS Options in an AAA Profile	190
Applying an AAA Profile to an APN	190
Enabling Address Assignment by the RADIUS Server	191
Configuring AAA-Assigned Addresses to Override Locally or DHCP-Assigned Addresses	191
Configuring the Broadband Gateway to Wait for an Accounting Response	192
Example: Configuring AAA on the Broadband Gateway	192

Chapter 8	Configuring DHCP	207
	DHCP Overview	207
	DHCP Protocol	207
	DHCP Proxy Client	208
	Configuring DHCP Proxy Client	208
	Configuring DHCP Under APN	209
Part 5	GPRS Tunneling Protocol (GTP) Configuration	
Chapter 9	Configuring GTP	213
	GTP Versions and GPRS Interfaces Overview	214
	GPRS Tunneling Protocol (GTP) Overview	216
	GTP Path Management Overview	216
	Default Path Management Configuration	217
	GTP Version Support for Echo Requests and Echo Responses	217
	Understanding Path Management	218
	Successful Echo-Request Sequence for Path Management	218
	Failed Echo Request Sequence for Path Management	219
	GTP Tunnel Management Overview	220
	GTP Tunnel Management Functions	220
	Default Tunnel Management Configuration	220
	GTP Version Support for Tunnel Management Requests and Responses	220
	Understanding Tunnel Management	221
	Successful Create Request Sequence for Tunnel Management	221
	Successful Update/Delete Request Sequence for Tunnel Management	222
	Failed Update/Delete Request Sequence for Tunnel Management	222
	Restart Counters Overview	223
	Understanding CSID Signaling	224
	Understanding Tunnel Endpoint Identifiers	225
	Configuring GTP Services Overview	226
	GTP-C and GTP-U Path Management	226
	Configuring GTP Services at Different Levels on a Broadband Gateway	226
	GTP Services Default Settings	227
	GTP Version Support	228
	Configuring a Loopback Interface for Transport of GTP Packets	228
	Configuring GTP Services on a Broadband Gateway	229
	Configuring GTP Services on the Control Plane	230
	Configuring GTP Services on the Data Plane	232
	Configuring GTP Services on the S5 Interface	233
	Configuring GTP Services on the S8 Interface	235
	Configuring GTP Services on the Gn Interface	236
	Configuring GTP Services on the Gp Interface	238
	Configuring GTP Services When the S5 and S8 Interfaces Are in Different VRFs	239
	Configuring GTP Services When the S5 and S8 Interfaces Are in the Same VRF	241
	Configuring GTP Services When 3GPP Interfaces Are in Different VRFs	242
	Configuring GTP Services on a GGSN Broadband Gateway	244
	Configuring GTP Services on a Peer Group	245

	Disabling Path Management on a Broadband Gateway or Peer Group	247
	Configuring GTP Trace Options	247
	Configuring General GTP Service on the S-GW	249
	Configuring GTP-C Services on the S11 Interface	252
	Configuring GTP-U Services on the S12 Interface	254
	Configuring GTP Services on the S1-U Interface	256
	Configuring GTP Services on the S4 Interface	257
	Configuring GTP Services on the S-GW When the S4 and S5 Interfaces Are in the Same VRF	259
	Configuring GTP Services on the S-GW When Interfaces are in Different VRFs	261
	Configuring S-GW GTP Traceoptions	262
	Example: Configuring GTP for the S-GW When Interfaces Are in different VRFs	265
Part 6	Charging Configuration	
Chapter 10	Charging Overview	271
	Charging	271
	Charging Services Overview	271
	Charging Data Records	273
	Information Collection and CDR Generation	275
	CDR Delivery	276
	Charging Profiles	277
	Charging Profile Selection Process	277
Chapter 11	Configuring Charging	279
	Configuring Charging	279
	Configuring S-GW-Specific Charging Parameters	280
	Configuring S-GW Global Charging Profiles and Selection Order	282
	Configuring S-GW Charging Traceoptions	284
	Configuring S-GW Local Persistent Storage Traceoptions	287
	Configuring GTP Prime for Charging	289
	Configuring GTP Prime for Transferring CDRs	289
	Configuring GTP Prime Peers	290
	Configuring Persistent Storage	291
	Configuring Local Persistent Storage	291
	Tracing Persistent Storage Operations	292
	Configuring the Solid State Disk for Persistent Storage	293
	Initializing the Solid State Disk for Persistent Storage	293
	Ejecting the Solid State Disk	294
	Installing the Solid State Disk	294
	Configuring Transport Profiles	295
	Configuring Charging Trigger Events	296
	Configuring CDR Attributes	298
	Configuring Charging Profiles	300
	Configuring Charging Profiles for APNs	301

	Tracing Charging Operations	302
	Configuring the Trace Log Filename	303
	Configuring the Tracing Flags	303
	Verifying and Managing the Charging Configuration	304
Part 7	Quality of Service Configuration	
Chapter 12	Configuring Quality of Service	309
	Quality of Service Overview	310
	Initial QoS	310
	Differentiated Services	310
	QoS Parameters in 3G Networks	311
	QoS Parameters in 4G Networks	312
	Aggregate Maximum Bit Rate	314
	Allocation and Retention Priority	314
	Preemption	314
	Call Admission Control Overview	315
	Enforcing Call Admission Control	315
	Managing Bandwidth	315
	Managing the Number of Bearers	316
	Managing Resource Thresholds	316
	Default Resource Threshold Settings	317
	Class of Service (CoS) Policy Profile Overview	317
	Policing Subscriber Traffic on the Broadband Gateway Overview	318
	Applying Rewrite Rules on Mobile Interfaces Overview	319
	Understanding Upstream and Downstream Processing of ToS Values in GTP-U	
	Packets	320
	Processing of ToS Values for Upstream Subscriber Packets	320
	Processing of ToS Values for Downstream Subscriber Packets	321
	Understanding How NQN and Upgrade Flags in PDP Contexts Affect QoS	
	Upgrade Behavior	321
	Configuring QoS on the Broadband Gateway Overview	323
	Configuring the Maximum Number of Bearers	324
	Configuring Bandwidth Pools	325
	Configuring Preemption for Call Admission Control	326
	Configuring Resource Thresholds on a 4G Network	326
	Configuring Resource Thresholds on a 3G Network	328
	Configuring Resource Thresholds for 3G and 4G Networks	330
	Configuring a Classifier Profile for a 4G Network	332
	Configuring a Classifier Profile for a 3G Network	333
	Configuring a Classifier Profile for 3G and 4G Networks	334
	Configuring a CoS Policy Profile for a 4G Network	336
	Configuring a CoS Policy Profile for a 3G Network	338
	Configuring a CoS Policy Profile for 3G and 4G Networks	340
	Configuring a Local Policy	343
	Applying a Local Policy	344
	Configuring Ingress Rewrite Rules for a Mobile Interface	345
	Configuring Egress Rewrite Rules for a Mobile Interface	345
	Applying Ingress Rewrite Rules to a Mobile Interface	346

	Applying Egress Rewrite Rules to Mobile Interfaces	347
	Example: Configuring Quality of Service	348
	Configuring S-GW-Specific CAC Parameters	384
	Example: Configuring QoS and CAC on a S-GW	385
Part 8	Maintenance	
Chapter 13	Maintenance Mode	393
	Mobility Maintenance Mode Overview	394
	Changing a GTP Interface Address	395
	Deleting a GTP Interface	396
	Modifying an Access Point Name	398
	Configuring the Mobile Interface of an Access Point Name	399
	Deleting an Access Point Name	401
	Changing a Charging Profile	402
	Changing a Transport Profile	403
	Changing a Trigger Profile	405
	Deleting a Charging Profile	406
	Changing a Call Detail Record Profile in a Charging Profile	407
	Changing Address Attributes in the Mobile Address Pool	408
	Deleting a Mobile Address Pool	410
	Example: Changing Access Point Name Values	411
	Example: Deleting an APN	412
	Example: Changing a Charging Profile	413
	Example: Changing a Transport Profile	415
	Example: Changing Mobility Pool Attributes	416
	Example: Deleting a Mobility Address Pool	422
	Example: Modifying Mobile Interface Parameters	423
Part 9	Monitoring and Troubleshooting	
Chapter 14	Monitoring	429
	Monitoring the Mobile Environment - Key Performance Indicators	429
	Monitoring Resources	430
	Monitoring GTP Signaling	430
	Monitoring Session Status	431
	Monitoring CPU Indicators	432
	Monitoring Memory Indicators	433
	Monitoring Charging Gateways	433
	Monitoring Data Path Measurements	435
	Monitoring Call Rate Statistics	435
	Monitoring Data Rate Statistics	435
	Tracing Control Packets	438
	How to Trace Data Packets from Gn to Gi Interfaces	442
	Trace Data Packets from Gi to Gn Interfaces	446
	How to Verify Charging Statistics Processing	453
Chapter 15	Troubleshooting	457
	Troubleshooting Overload Conditions in the Mobile Network	457
	Troubleshooting Multilevel Overload Protection	457

	Responding to an Overload	458
	Monitoring GTP Signaling	458
	Troubleshooting Alarms, Logs, and Traps	459
	Troubleshooting Admission Control	461
	Monitoring AAA Metrics	463
Part 10	Examples	
Chapter 16	Example Configurations	471
	Example: Simple Unified Edge Configuration	471
	Example: Configuring MobileNext Broadband Gateway	479
	Example: Configuring MobileNext Broadband Gateway with Provider Edge Functionality	507
	Example: Configuring NAT	516
	Example: Configuring a Standalone S-GW	519
	Example: Configuring a Collocated P-GW and S-GW	525
	Example: Configuring a Multigateway P-GW and S-GW	535
Part 11	Complete Configuration Statement Hierarchy and Summary of Statements	
Chapter 17	Configuration Statement Hierarchy	553
	[edit access] Hierarchy Level	553
	[edit access address-assignment] Hierarchy Level	554
	[edit class-of-service] Hierarchy Level	555
	[edit interfaces ams] Hierarchy Level	555
	[edit interfaces apfe] Hierarchy Level	556
	[edit interfaces mif] Hierarchy Level	557
	[edit routing-instance system] Hierarchy Level	557
	[edit services hcm] Hierarchy Level	558
	[edit services ip-reassembly] Hierarchy Level	559
	[edit services service-set] Hierarchy Level	559
	[edit unified-edge] Hierarchy Level	559
	[edit unified-edge aaa] Hierarchy Level	560
	[edit unified-edge cos-cac] Hierarchy Level	561
	[edit unified-edge gateways] Hierarchy Level	563
	[edit unified-edge gateways ggsn-pgw <gateway-name>] Hierarchy Level	564
	[edit unified-edge gateways sgw <gateway-name>] Hierarchy Level	574
	[edit unified-edge local-policies] Hierarchy Level	582
	[edit unified-edge mobile-options] Hierarchy Level	582
	[edit unified-edge resource-management] Hierarchy Level	582
Chapter 18	AAA on the Broadband Gateway	585
	aaa	586
	accounting	588
	accounting-port	589
	accounting-secret	589
	address	590
	algorithm	590
	allow-dynamic-requests	591

	attributes	592
	authentication	593
	authentication-port	593
	dead-criteria-retries	594
	dynamic-requests-secret	594
	exclude (RADIUS)	595
	ignore	597
	maximum-pending-reqs-limit	597
	mobile-profiles	598
	network-element	600
	network-element-group	600
	network-element-groups	601
	network-elements	602
	options	603
	radius (Access)	604
	radius	606
	retry	608
	revert-interval	608
	secret	609
	send-accounting-on	609
	servers	610
	source-interface	611
	stop-on-access-deny	611
	stop-on-failure	612
	timeout	612
	traceoptions	613
	traceoptions	614
	trigger	615
Chapter 19	Address Assignment and DHCP Configuration Statements	617
	Address Assignment Configuration Statements	618
	address-assignment (MobileNext Broadband Gateway)	618
	ageing-window (Mobile Pools)	619
	default-pool (Mobile Pools)	619
	external-assigned (Mobile Pools)	620
	family (Mobile Pools)	621
	mobile-pool-groups	622
	mobile-pools	623
	network (Mobile Pools)	624
	pool-prefetch-threshold (Mobile Pools)	625
	pool-snmp-trap-threshold (Mobile Pools)	626
	range (Mobile Pools)	627
	service-mode (Mobile Pools)	628
	DHCP Configuration Statements	629
	bind-interface	629
	dead-server-retry-interval	630
	dead-server-successive-retry-attempt	631
	dhcp-proxy-client	632
	dhcp-server-selection-algorithm	633

	dhcpv4-profiles	634
	dhcpv6-profiles	635
	lease-time	636
	pool-name	636
	priority	637
	retransmission-attempt	638
	retransmission-interval	639
	server	640
	services	641
	system	642
	trace-options	643
Chapter 20	Anchor Packet Forwarding Engine Redundancy and Aggregated Multiservices High Availability Configuration Statements	645
	anchor-pfes	645
	anchor-service-pics	646
	anchor-spics	646
	anchoring-options (Aggregated Packet Forwarding Engine)	647
	apfe-group-set (Aggregated Packet Forwarding Engine)	648
	dedicated (IPsec)	649
	dial-options (IPsec)	649
	drop-member-traffic (Aggregated Multiservices)	650
	enable-rejoin (Aggregated Multiservices)	651
	family (Aggregated Multiservices)	652
	high-availability-options (Aggregated Multiservices)	653
	interface (Anchor Packet Forwarding Engine)	654
	interface (Services PIC)	656
	interface (Session PIC)	657
	interfaces (Aggregated Multiservices)	658
	interfaces (Aggregated Packet Forwarding Engine)	660
	ipsec-interface-id (IPsec)	661
	load-balancing-options (Aggregated Multiservices)	662
	load-balancing-options (IPsec)	663
	many-to-one (Aggregated Multiservices)	664
	member-failure-options (Aggregated Multiservices)	665
	member-interface (Aggregated Multiservices)	667
	preferred-active (IPsec)	668
	primary-list (Aggregated Packet Forwarding Engine)	669
	redistribute-all-traffic (Aggregated Multiservices)	670
	rejoin-timeout (Aggregated Multiservices)	671
	secondary (Aggregated Packet Forwarding Engine)	672
	shared (IPsec)	672
	system	673
	unit (Aggregated Multiservices)	674
	warm-standby (Aggregated Packet Forwarding Engine)	675
Chapter 21	APN Configuration Statements	677
	APN Services Configuration Statements	677
	aaa (APN Address Assignment)	677
	aaa-override (APN Address Assignment)	678

aaa-profile (APN)	679
address-assignment (APN)	680
allow-network-behind-mobile	681
allow-static-ip-address (APN Address Assignment)	682
anchor-pfe-ipv4-nbm-prefixes	683
anchor-pfe-ipv6-nbm-prefixes	684
anonymous-user (APN)	685
apn-data-type	686
apn-services	687
apn-type	690
apns	691
block-visitors	693
count (HTTP Header Enrichment)	694
charging (APN)	695
default-profile	697
description (APN)	698
destination-address (HTTP Header Enrichment)	698
destination-address-range (HTTP Header Enrichment)	699
destination-port-range (HTTP Header Enrichment)	699
destination-ports (HTTP Header Enrichment)	700
destination-prefix-list (HTTP Header Enrichment)	701
dhcp-proxy-client (APN Address Assignment)	702
dhcpv4-proxy-client-profile (APN Address Assignment)	703
dhcpv6-proxy-client-profile (APN Address Assignment)	704
dns-server (APN)	705
encrypt (HTTP Header Enrichment)	706
exclude-pools (APN Address Assignment)	707
exclude-v6pools (APN Address Assignment)	708
from (HTTP Header Enrichment)	709
group (APN Address Assignment)	710
hcm (HTTP Header Enrichment)	711
home-profile	712
idle-timeout (APN)	713
idle-timeout-direction (APN)	714
imsi (Network Behind Mobile)	715
inet-pool (APN Address Assignment)	716
inet6-pool (APN Address Assignment)	717
inter-mobile-traffic (APN)	718
local (APN Address Assignment)	719
local-policy-profile (APN)	720
logical-system (APN Address Assignment)	721
maximum-bearers (APN)	722
mobile-interface (APN)	723
nbns-server (APN)	724
network-behind-mobile	725
no-address-verify (APN Address Assignment)	725
p-cscf (APN)	726
prefix-v4 (Network Behind Mobile)	727
prefix-v6 (Network Behind Mobile)	728

pool (APN Address Assignment)	729
pool-name (APN Address Assignment)	730
profile-name (APN Address Assignment)	731
profile-selection-order (APN)	732
restriction-value (APN)	733
roamer-profile	734
routing-instance (APN Address Assignment)	735
rule (Tag Rule Set)	736
selection-mode (APN)	737
service-mode (APN)	738
service-selection-profile (APN)	739
service-set-options	739
session-timeout (APN)	740
subscriber-awareness (Service Set Options)	741
tag (HTTP Header Enrichment)	742
tag-attribute (HTTP Header Enrichment)	743
tag-attribute (HTTP Header Enrichment Tag)	743
tag-header (HTTP Header Enrichment)	744
tag-rule (HTTP Header Enrichment)	745
tag-rules (HTTP Header Enrichment)	746
tag-rule-set (HTTP Header Enrichment)	747
tag-rule-sets (HTTP Header Enrichment)	748
tag-separator (HTTP Header Enrichment)	748
term (HTTP Header Enrichment)	749
then (HTTP Header Enrichment)	750
verify-source-address (APN)	751
visitor-profile	752
wait-accounting (APN)	753
Service Selection Profiles Configuration Statements	754
apn-name (Service Selection Profiles)	754
charging-characteristics (Service Selection Profiles)	755
from (Service Selection Profiles)	756
imei (Service Selection Profiles)	757
imsi (Service Selection Profiles)	758
maximum-bearers (Service Selection Profiles)	759
msisdn (Service Selection Profiles)	760
pdn-type (Service Selection Profiles)	761
peer (Service Selection Profiles)	761
peer-routing-instance (Service Selection Profiles)	762
profile (Service Selection Profiles)	763
redirect-peer (Service Selection Profiles)	764
service-selection-profiles	765
term (Service Selection Profiles)	766
then (Service Selection Profiles)	767
Chapter 22 Charging Configuration Statements	769
cdr-aggregation-limit	769
cdr-profile	770
cdr-profiles	772

cdr-release	773
cdrs-per-file	774
charging	775
charging-gateways	779
charging-profiles	780
container-limit	781
default-profile	782
default-rating-group	783
default-service-id	784
description	785
destination-ipv4-address (GTP Prime)	786
destination-port (GTP Prime)	787
direction (Trigger Profiles)	788
disable-replication	789
disk-space-policy	790
down-detect-time (GTP Prime)	791
echo-interval (GTP Prime)	792
enable-reduced-partial-cdrs	793
exclude (Trigger Profiles)	794
exclude-ie-options	797
file-age	801
file-creation-policy	802
file-format	803
file-name-private-extension	804
file-size	805
global-profile (Serving Gateway)	806
gtp	807
header-type (GTP Prime)	808
home-profile	809
local-persistent-storage-options	810
local-storage	811
mtu (Transport Profiles)	812
n3-requests (GTP Prime)	813
no-path-management (GTP Prime)	814
offline (Transport Profiles)	815
offline (Trigger Profiles)	816
peer (GTP Prime)	817
peer (Peer Order)	818
peer-order	819
pending-queue-size (GTP Prime)	820
persistent-storage-order	821
profile-id	822
profile-selection-order (Serving Gateway)	823
reconnect-time (GTP Prime)	824
roamer-profile	825
service-mode (Charging Profiles)	826
service-mode (Transport Profiles)	828
sgsn-mme-change-limit (Serving Gateway)	829
sgsn-sgw-change-limit (GGSN or P-GW)	830

	source-interface (GTP Prime)	831
	switch-back-time	832
	t3-response (GTP Prime)	833
	tariff-time-list	834
	time-limit	835
	traceoptions (Charging)	836
	traceoptions (Local Persistent Storage)	839
	transport-profile	841
	transport-profiles	843
	transport-protocol (GTP Prime)	844
	trigger-profile	845
	trigger-profiles	846
	user-name (Local Persistent Storage)	847
	version (GTP Prime)	848
	visitor-profile	849
	volume-limit	850
	watermark-level-1	851
	watermark-level-2	852
	watermark-level-3	853
	world-readable (Local Persistent Storage)	854
Chapter 23	Class of Service (CoS) Configuration Statements	855
	aggregated-maximum-bit-rate	855
	allocation-retention-priority	856
	anchor-pfe-default-bearers-percentage (Serving Gateway)	857
	anchor-pfe-guaranteed-bandwidth (Serving Gateway)	858
	anchor-pfe-maximum-bearers (Serving Gateway)	859
	bandwidth-pools	860
	bearer-load	861
	classifier-profile	862
	classifier-profiles	863
	class-of-service	864
	cos-cac	865
	cos-policy-profile	867
	cos-policy-profiles	868
	cpu	869
	dl-bandwidth-pool	870
	dscp-ipv6	870
	dscp-ipv6 (Ingress)	871
	dscp	871
	dscp (Ingress)	872
	exceed-action	872
	guaranteed-bit-rate	873
	high	874
	inet-precedence	874
	inet-precedence (Ingress)	875
	ingress-rewrite-rules	875
	interfaces	876
	local-policies	877

	local-policy-profile (Broadband Gateway)	878
	low	879
	maximum-bearers (Broadband Gateway)	880
	maximum-bit-rate	881
	memory	882
	mif	883
	preemption (GGSN or P-GW)	884
	preemption (Serving Gateway)	885
	qos-class-identifier	886
	resource-threshold-profiles	887
	resource-threshold-profile	888
	rewrite-rules	889
	roamer-classifier-profile	889
	roamer-cos-policy-profile	890
	system-load	891
	traffic-class-classifier-profiles	892
	traffic-class-cos-policy-profiles	893
	ul-bandwidth-pool	894
	violate-action	894
	visitor-classifier-profile	895
	visitor-cos-policy-profile	895
Chapter 24	Exception Handling Configuration Statements	897
	current-hop-limit (IPv6 Router Advertisement)	897
	disable (IPv6 Router Advertisement)	898
	error-indication-interval	898
	ip-reassembly	899
	ip-reassembly-profile	900
	ipv6-router-advertisement (MobileNext Broadband Gateway)	901
	max-reassembly-pending-packets (IP Reassembly)	902
	maximum-advertisement-interval (IPv6 Router Advertisement)	903
	maximum-initial-advertisement-interval (IPv6 Router Advertisement)	904
	maximum-initial-advertisements (IPv6 Router Advertisement)	905
	minimum-advertisement-interval (IPv6 Router Advertisement)	906
	reachable-time (IPv6 Router Advertisement)	907
	retransmission-timer (IPv6 Router Advertisement)	908
	router-lifetime (IPv6 Router Advertisement)	909
	software-datapath	910
	timeout (IP Reassembly)	911
	traceoptions (Exception Handling)	912
Chapter 25	Gateway Maintenance Mode Configuration Statement	915
	service-mode (GGSN or P-GW)	915
	service-mode (Serving Gateway)	916
Chapter 26	GTP Configuration Statements	917
	control (GTP)	917
	control (GTP Gn, Gp, S4, S5, and S8 Interfaces)	918
	control (Peer Group)	919
	data (GTP)	920

	data (GTP Gn, Gp, S4, S5, and S8 Interfaces)	921
	ddn-delay-sync	922
	dscp-code-point (GTP)	923
	echo-interval (GTP)	924
	echo-n3-requests	926
	echo-t3-response	928
	error-indication-interval	930
	forwarding-class (GTP)	931
	gn	932
	gp	934
	gtp (GGSN or P-GW)	936
	gtp (S-GW)	941
	indirect-tunnel	945
	interface (GTP)	946
	n3-requests	948
	no-response-cache	949
	num-gtpu-end-markers	950
	path-management	951
	peer (GTP)	952
	peer-group (GTP)	953
	peer-history (GTP)	954
	response-cache-timeout	955
	routing-instance (GTP)	956
	s11	957
	s12	958
	s1u	959
	s4	960
	s5	962
	s8	964
	support-16-bit-sequence	965
	t3-response	966
	traceoptions (GTP)	968
	tth-value (S-GW GTP-C)	970
Chapter 27	Service Applications Configuration Statements	971
	egress-key (Aggregated Multiservices)	971
	hash-keys (Aggregated Multiservices)	972
	ingress-key (Aggregated Multiservices)	974
	interface-service (Aggregated Multiservices)	975
	load-balancing-options (Aggregated Multiservices for Services Applications)	976
	resource-triggered (Aggregated Multiservices)	977
	service-set (Aggregated Multiservices)	978
Chapter 28	System Architecture and Gateway Traceoptions Configuration Statements	981
	System Architecture Configuration Statements	981
	call-rate-statistics	981
	disable (Idle Mode Buffering)	982
	expire-timer (Idle Mode Buffering)	983

family (Mobile Interface)	983
filter (Mobile Interface)	984
forwarding-packages	985
ggsn-pgw	986
history (Call-Rate Statistics)	986
home-plmn	987
idle-mode-buffering	988
input (Mobile Interface)	988
interface	989
interfaces (Mobile Interface)	990
interval (Call-Rate Statistics)	991
local-policy-profile (Broadband Gateway)	992
maximum-bearers (Broadband Gateway)	993
mcc	994
mnc	995
mobility	996
mtu (Mobile Interface)	997
output (Mobile Interface)	997
remote-delete-on-peer-fail	998
sgw	998
unit (Mobile Interface)	999
Gateway Traceoptions Configuration Statements	1000
client (Resource Management)	1000
mobile-options	1001
resource-management (MobileNext Broadband Gateway)	1002
server (Resource Management)	1003
traceoptions (Broadband Gateway)	1004
traceoptions (Mobile Options)	1007
traceoptions (Resource Management Client)	1009
traceoptions (Resource Management Server)	1012

Part 12

Chapter 29

Command Reference

AAA Operational Commands	1017
clear unified-edge ggsn-pgw aaa radius statistics	1018
clear unified-edge ggsn-pgw aaa statistics	1019
clear unified-edge ggsn-pgw address-assignment pool	1020
clear unified-edge ggsn-pgw address-assignment statistics	1021
show unified-edge ggsn-pgw aaa network-element status	1022
show unified-edge ggsn-pgw aaa network-element-group status	1024
show unified-edge ggsn-pgw aaa radius statistics	1026
show unified-edge ggsn-pgw aaa statistics	1035
show unified-edge ggsn-pgw address-assignment group	1041
show unified-edge ggsn-pgw address-assignment pool	1044
show unified-edge ggsn-pgw address-assignment service-mode	1048
show unified-edge ggsn-pgw address-assignment statistics	1050

Chapter 30	Anchor Packet Forwarding Engine Redundancy and Aggregated Multiservices High Availability Operational Commands	1053
	request interface load-balancing revert (Aggregated Multiservices)	1054
	request interface load-balancing switchover (Aggregated Multiservices)	1055
	show interfaces anchor-group (Aggregated Packet Forwarding Engine)	1056
	show interfaces load-balancing (Aggregated Multiservices)	1059
	show services ipsec-vpn ipsec security-associations	1062
	show unified-edge ggsn-pgw system interfaces	1066
	show unified-edge sgw system interfaces	1068
Chapter 31	APN and Related Operational Commands	1071
	show services hcm statistics	1072
	clear unified-edge ggsn-pgw statistics	1074
	clear unified-edge ggsn-pgw subscribers	1075
	clear unified-edge ggsn-pgw subscribers charging	1077
	clear unified-edge ggsn-pgw subscribers peer	1078
	show unified-edge ggsn-pgw apn service-mode	1079
	show unified-edge ggsn-pgw apn statistics	1081
	show unified-edge ggsn-pgw service-mode	1086
	show unified-edge ggsn-pgw statistics	1088
	show unified-edge ggsn-pgw status	1091
	show unified-edge ggsn-pgw subscribers	1095
	show unified-edge ggsn-pgw subscribers charging	1105
Chapter 32	Charging Operational Commands	1109
	clear unified-edge ggsn-pgw charging cdr	1110
	clear unified-edge ggsn-pgw charging cdr wfa	1111
	clear unified-edge ggsn-pgw charging local-persistent-storage statistics	1112
	clear unified-edge ggsn-pgw charging path statistics	1113
	clear unified-edge ggsn-pgw charging transfer statistics	1114
	clear unified-edge sgw charging cdr	1115
	clear unified-edge sgw charging local-persistent-storage statistics	1116
	clear unified-edge sgw charging path statistics	1117
	clear unified-edge sgw charging transfer statistics	1118
	request system storage unified-edge charging media start	1119
	request system storage unified-edge charging media stop	1120
	request system storage unified-edge media eject	1121
	request system storage unified-edge media prepare	1122
	show unified-edge ggsn-pgw charging local-persistent-storage statistics	1123
	show unified-edge ggsn-pgw charging path statistics	1128
	show unified-edge ggsn-pgw charging path status	1133
	show unified-edge ggsn-pgw charging service-mode	1136
	show unified-edge ggsn-pgw charging transfer statistics	1139
	show unified-edge ggsn-pgw charging transfer status	1143
	show unified-edge ggsn-pgw charging trigger-profile	1146
	show unified-edge sgw charging local-persistent-storage statistics	1148
	show unified-edge sgw charging path statistics	1154
	show unified-edge sgw charging path status	1159
	show unified-edge sgw charging service-mode	1162

	show unified-edge sgw charging transfer statistics	1164
	show unified-edge sgw charging transfer status	1168
	show unified-edge sgw charging trigger-profile	1170
Chapter 33	Class of Service (CoS) Operational Commands	1173
	show unified-edge ggsn-pgw qos statistics	1174
	show unified-edge ggsn-pgw status preemption-list	1177
	show unified-edge sgw status preemption-list	1180
Chapter 34	Exception Handling Operational Commands	1183
	clear unified-edge ggsn-pgw ip-reassembly statistics	1184
	clear unified-edge sgw ip-reassembly statistics	1185
	show unified-edge ggsn-pgw ip-reassembly statistics	1186
	show unified-edge sgw ip-reassembly statistics	1189
Chapter 35	GPRS Tunneling Protocol (GTP) Operational Commands	1193
	clear unified-edge ggsn-pgw gtp peer statistics	1194
	clear unified-edge ggsn-pgw gtp statistics	1196
	clear unified-edge sgw gtp peer statistics	1197
	clear unified-edge sgw gtp statistics	1198
	show unified-edge ggsn-pgw gtp peer	1199
	show unified-edge ggsn-pgw gtp peer statistics	1203
	show unified-edge ggsn-pgw gtp statistics	1211
	show unified-edge sgw gtp peer	1221
	show unified-edge sgw gtp peer statistics	1225
	show unified-edge sgw gtp statistics	1230
Chapter 36	Service Applications Operational Commands	1237
	show services flows (Aggregated Multiservices)	1238
	show services nat mappings app	1242
	show services nat mappings eim	1244
	show services nat mappings summary	1246
	show services nat pool (Aggregated Multiservices)	1247
	show services nat statistics	1250
	show services service-sets summary	1259
	show services sessions (Aggregated Multiservices)	1261
Chapter 37	System Architecture Operational Commands	1269
	clear unified-edge sgw idle-mode-buffering statistics	1270
	clear unified-edge sgw statistics	1271
	clear unified-edge sgw subscribers	1272
	clear unified-edge sgw subscribers charging	1273
	clear unified-edge sgw subscribers peer	1274
	show unified-edge gateways	1275
	show unified-edge ggsn-pgw call-rate statistics	1277
	show unified-edge ggsn-pgw resource-manager clients	1280
	show unified-edge sgw call-rate statistics	1282
	show unified-edge sgw service-mode	1284
	show unified-edge sgw idle-mode-buffering statistics	1286
	show unified-edge sgw resource-manager clients	1290
	show unified-edge sgw statistics	1292

show unified-edge sgw status	1295
show unified-edge sgw subscribers	1300
show unified-edge sgw subscribers charging	1308

Part 13

Index

Index	1315
Index of Statements and Commands	1337

List of Figures

Part 1	Overview	
Chapter 1	System Architecture	3
	Figure 1: The Broadband Gateway System Architecture	4
	Figure 2: Broadband Gateway GTP Signaling Packet Flow	6
	Figure 3: Broadband Gateway Uplink User Packet Flow	7
	Figure 4: Broadband Gateway Downlink User Packet Flow	9
	Figure 5: S-GW Interfaces on the Broadband Gateway	22
	Figure 6: S-GW and the S1 and X2 Interfaces	24
	Figure 7: GTP-U Packet Flow Through Standalone S-GW	25
	Figure 8: Collocated Gateways S-GW and P-GW Resources and Load Balancing	26
	Figure 9: Collocated S-GW and P-GW Control Packet Flow	28
	Figure 10: Collocated S-GW and P-GW User Packet Flow	29
Chapter 2	Network Architecture	37
	Figure 11: 3G Mobile Network Architecture	39
	Figure 12: 4G/LTE Mobile Network Basic Components	41
	Figure 13: Packet Data Network Gateway Functions	42
	Figure 14: Major Components of the Evolved Packet Core	44
	Figure 15: APNs and the P-GW	46
	Figure 16: Bearers, Gateways, and Packet Networks	48
	Figure 17: The GGSN in a 3G Network	49
	Figure 18: LTE Network Deployment Scenario	51
	Figure 19: S1 Interface Is Many-to-Many	53
	Figure 20: Tracking Areas and the S1 Interface	54
	Figure 21: S-GW Functions	56
Part 2	System Configuration	
Chapter 3	Configuring Mobility on MX 3D Devices	61
	Figure 22: Session DPCs and Interfaces on the Broadband Gateway	62
	Figure 23: Upstream GTP-U Traffic	70
	Figure 24: Downstream GTP-U Traffic	70
Chapter 4	Configuring Redundancy on MX 3D Devices	73
	Figure 25: Redundancy Available on the Broadband Gateway	74
	Figure 26: Control Plane Anchor Operation Before Failure	80
	Figure 27: Control Plane Anchor Operation After Failure	81
	Figure 28: Pre- and Post-Failure PFE Datapaths	81
	Figure 29: Redundancy Example for the Broadband Gateway	83
Chapter 5	Configuring Mobile Edge Exception Handling	87

	Figure 30: GTP-C Handling	88
Part 3	APN Configuration	
Chapter 6	Configuring APNs	105
	Figure 31: APNs and P-GWs in the 4G Architecture	106
	Figure 32: APNs Connect Mobile Devices to IP Networks Through a P-GW	127
	Figure 33: Network That Is Behind the Mobile Device and the P-GW	130
Part 5	GPRS Tunneling Protocol (GTP) Configuration	
Chapter 9	Configuring GTP	213
	Figure 34: GTP Versions Supported on a MobileNext Broadband Gateway	214
	Figure 35: GTP-C Versions Supported for 3G/4G Network Interfaces	215
	Figure 36: Successful Echo-Request Sequence for Path Management	218
	Figure 37: Failed Echo-Request Sequence for Path Management	219
	Figure 38: Successful Create Request Sequence for Tunnel Management	221
	Figure 39: Successful Update/Delete Request Sequence for Tunnel Management	222
	Figure 40: Failed Update/Delete Request Sequence for Tunnel Management	223
	Figure 41: GTP-C Performs Signaling Between the Serving Gateway and Packet Data Network Gateway	225
Part 6	Charging Configuration	
Chapter 10	Charging Overview	271
	Figure 42: Simple Charging Topology	272
Part 7	Quality of Service Configuration	
Chapter 12	Configuring Quality of Service	309
	Figure 43: Key QoS Parameters for PDP Context Requests	312
	Figure 44: Key QoS Parameters for 4G Default Bearer Requests	313
	Figure 45: QoS Negotiation Behavior for PDP Contexts with NQN and Upgrade Flags	322

List of Tables

	About This Guide	xxxv
	Table 1: Notice Icons	xxxix
	Table 2: Text and Syntax Conventions	xxxix
Part 1	Overview	
Chapter 1	System Architecture	3
	Table 3: General Gateway Trace Flags	15
	Table 4: Trace Levels	15
	Table 5: Mobile Options Trace Flags	17
	Table 6: Trace Levels	17
	Table 7: Resource Management Server Trace Flags	19
	Table 8: Resource Management Client Trace Flags	20
	Table 9: Trace Levels	20
	Table 10: S-GW Trace Flags	33
	Table 11: S-GW Trace Levels	33
Part 2	System Configuration	
Chapter 5	Configuring Mobile Edge Exception Handling	87
	Table 12: Trace Flags	95
	Table 13: Trace Levels	95
	Table 14: S-GW Data Path Trace Flags	97
	Table 15: S-GW Datapath Trace Levels	97
Part 3	APN Configuration	
Chapter 6	Configuring APNs	105
	Table 16: APN Restriction Values	114
Part 4	Authorization and Addressing Configuration	
Chapter 7	Configuring AAA	147
	Table 17: RADIUS IETF Attributes Supported in Access-Request Messages	155
	Table 18: 3GPP VSAs Supported in Access-Request Messages	157
	Table 19: RADIUS IETF Attributes Supported in Access-Accept Messages	160
	Table 20: 3GPP VSAs Supported in Access-Accept Messages	161
	Table 21: Juniper VSAs Supported in Access-Accept Messages	162
	Table 22: RADIUS IETF Attributes Supported in Accounting Start Messages	163
	Table 23: 3GPP VSAs Supported in Accounting Start Messages	164

	Table 24: RADIUS IETF Attributes Supported in Accounting Interim-Update Messages	167
	Table 25: 3GPP VSAs Supported in Accounting Interim-Update Messages	169
	Table 26: RADIUS IETF Attributes Supported in Accounting Stop Messages	171
	Table 27: 3GPP VSAs Supported in Accounting Stop Messages	173
	Table 28: RADIUS IETF Attributes Supported in Accounting On Messages	176
	Table 29: RADIUS IETF Attributes Supported in Disconnect Request Messages	176
	Table 30: 3GPP VSAs Supported in Disconnect Request Messages	177
	Table 31: RADIUS IETF Attributes Supported in CoA Messages	178
	Table 32: 3GPP VSAs Supported in CoA Messages	178
	Table 33: Events You Can Exclude from Triggering Interim-Update Messages	185
	Table 34: RADIUS Attributes the Broadband Gateway Can Ignore in Accept-Accept Messages	187
	Table 35: RADIUS Attributes the Broadband Gateway Can Exclude from RADIUS Messages	187
	Table 36: 3GPP VSAs That Can Be Excluded from RADIUS Messages	188
Part 5	GPRS Tunneling Protocol (GTP) Configuration	
Chapter 9	Configuring GTP	213
	Table 37: Trace Flags	247
	Table 38: Trace Levels	248
	Table 39: S-GW GTP Trace Flags	263
	Table 40: S-GW GTP Trace Levels	263
	Table 41: Components of the Broadband Gateway	265
Part 6	Charging Configuration	
Chapter 11	Configuring Charging	279
	Table 42: S-GW Charging Trace Flags	284
	Table 43: S-GW Charging Trace Levels	285
	Table 44: S-GW Local Persistent Storage Trace Flags	287
	Table 45: S-GW Local Persistent Storage Trace Levels	287
Part 7	Quality of Service Configuration	
Chapter 12	Configuring Quality of Service	309
	Table 46: Traffic Classes for a 3G Network	311
	Table 47: QoS Class Identifier for a 4G Network	312
Part 10	Examples	
Chapter 16	Example Configurations	471
	Table 48: Unified Edge — Simple Configuration	472
	Table 49: Components of the Broadband Gateway	479
	Table 50: Components of the Broadband Gateway	508

Part 11	Complete Configuration Statement Hierarchy and Summary of Statements	
Chapter 20	Anchor Packet Forwarding Engine Redundancy and Aggregated Multiservices High Availability Configuration Statements	645
	Table 51: Behavior of Member Interface After One Multiservices PIC Fails	665
	Table 52: Behavior of Member Interface After Two Multiservices PICs Fail	666
Chapter 21	APN Configuration Statements	677
	Table 53: Valid Restriction Values for APNs	733
	Table 54: Selection Mode Values	737
Chapter 22	Charging Configuration Statements	769
	Table 55: Triggers and Corresponding IEs	795
Chapter 27	Service Applications Configuration Statements	971
	Table 56: Hash Keys Supported for AMS for Service Applications	973
Part 12	Command Reference	
Chapter 29	AAA Operational Commands	1017
	Table 57: show unified-edge ggsn-pgw aaa network-element status Output Fields	1022
	Table 58: show unified-edge ggsn-pgw aaa network-element-group status Output Fields	1024
	Table 59: show unified-edge ggsn-pgw aaa radius statistics Output Fields	1027
	Table 60: show unified-edge ggsn-pgw aaa statistics Output Fields	1036
	Table 61: show unified-edge ggsn-pgw address-assignment-group Output Fields	1041
	Table 62: show unified-edge ggsn-pgw address-assignment pool Output Fields	1045
	Table 63: show unified-edge ggsn-pgw address-assignment service-mode Output Fields	1048
	Table 64: show unified-edge ggsn-pgw address-assignment statistics Output Fields	1050
Chapter 30	Anchor Packet Forwarding Engine Redundancy and Aggregated Multiservices High Availability Operational Commands	1053
	Table 65: show interfaces anchor-group	1056
	Table 66: show interfaces load-balancing Output Fields	1059
	Table 67: show services ipsec-vpn ipsec security-associations Output Fields	1062
	Table 68: show unified-edge ggsn-pgw system interfaces	1066
	Table 69: show unified-edge sgw system interfaces Output Fields	1068
Chapter 31	APN and Related Operational Commands	1071
	Table 70: show services hcm statistics Output Fields	1072
	Table 71: show unified-edge ggsn-pgw apn service-mode Output Fields	1079
	Table 72: show unified-edge ggsn-pgw apn statistics Output Fields	1081
	Table 73: show unified-edge ggsn-pgw service-mode Output Fields	1086
	Table 74: show unified-edge ggsn-pgw statistics Output Fields	1088
	Table 75: show unified-edge ggsn-pgw status Output Fields	1092

	Table 76: show unified-edge ggsn-pgw subscribers Output Fields	1097
Chapter 32	Charging Operational Commands	1109
	Table 77: show unified-edge ggsn-pgw charging local-persistent-storage statistics Output Fields	1123
	Table 78: show unified-edge ggsn-pgw charging path statistics Output Fields	1129
	Table 79: show unified-edge ggsn-pgw charging path status Output Fields . . .	1134
	Table 80: show unified-edge ggsn-pgw charging service-mode Output Fields	1136
	Table 81: show unified-edge ggsn-pgw charging transfer statistics Output Fields	1139
	Table 82: show unified-edge ggsn-pgw charging transfer status Output Fields	1143
	Table 83: show unified-edge ggsn-pgw charging trigger-profile Output Fields	1146
	Table 84: show unified-edge sgw charging local-persistent-storage statistics Output Fields	1148
	Table 85: show unified-edge sgw charging path statistics Output Fields	1155
	Table 86: show unified-edge sgw charging path status Output Fields	1160
	Table 87: show unified-edge sgw charging service-mode Output Fields	1162
	Table 88: show unified-edge sgw charging transfer statistics Output Fields . . .	1164
	Table 89: show unified-edge sgw charging transfer status Output Fields	1168
	Table 90: show unified-edge sgw charging trigger-profile Output Fields	1170
Chapter 33	Class of Service (CoS) Operational Commands	1173
	Table 91: show unified-edge ggsn-pgw qos statistics Output Fields	1174
	Table 92: show unified-edge ggsn-pgw status preemption-list Output Fields . .	1178
	Table 93: show unified-edge sgw status preemption-list Output Fields	1181
Chapter 34	Exception Handling Operational Commands	1183
	Table 94: show unified-edge ggsn-pgw ip-reassembly statistics Output Fields	1186
	Table 95: show unified-edge sgw ip-reassembly statistics Output Fields	1189
Chapter 35	GPRS Tunneling Protocol (GTP) Operational Commands	1193
	Table 96: show unified-edge ggsn-pgw gtp peer Output Fields	1200
	Table 97: show unified-edge sgw gtp statistics Output Fields	1212
	Table 98: show unified-edge sgw gtp peer Output Fields	1222
	Table 99: show unified-edge sgw gtp statistics Output Fields	1230
Chapter 36	Service Applications Operational Commands	1237
	Table 100: show services flows Output Fields	1240
	Table 101: show services nat mappings app Output Fields	1242
	Table 102: show services nat mappings eim Output Fields	1244
	Table 103: show services nat mappings summary Output Fields	1246
	Table 104: show services nat pool Output Fields	1247
	Table 105: show services nat statistics Output Fields	1250
	Table 106: show services service-sets summary Output Fields	1259
	Table 107: show services sessions Output Fields	1263
Chapter 37	System Architecture Operational Commands	1269

Table 108: show unified-edge gateways Field Descriptions	1275
Table 109: show unified-edge ggsn-pgw call-rate statistics Output Fields . . .	1277
Table 110: show unified-edge gateways ggsn-pgw resource-manager clients Output Fields	1280
Table 111: show unified-edge sgw call-rate statistics Output Fields	1282
Table 112: show unified-edge sgw service-mode Output Fields	1284
Table 113: show unified-edge sgw idle-mode-buffering statistics Output Fields	1286
Table 114: show unified-edge sgw resource-manager clients Output Fields . .	1290
Table 115: show unified-edge sgw statistics Output Fields	1292
Table 116: show unified-edge sgw status Output Fields	1296
Table 117: show unified-edge sgw subscribers Output Fields	1301

About This Guide

This preface provides the following guidelines for using the *MobileNext Broadband Gateway Configuration Guide*:

- [Junos Documentation and Release Notes on page xxxv](#)
- [Objectives on page xxxvi](#)
- [Audience on page xxxvi](#)
- [Supported Platforms on page xxxvi](#)
- [Using the Indexes on page xxxvii](#)
- [Using the Examples in This Manual on page xxxvii](#)
- [Documentation Conventions on page xxxviii](#)
- [Documentation Feedback on page xl](#)
- [Requesting Technical Support on page xl](#)

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

Using the Indexes

This reference contains two indexes: a complete index that includes topic entries, and an index of statements and commands only.

In the index of statements and commands, an entry refers to a statement summary section only. In the complete index, the entry for a configuration statement or command contains at least two parts:

- The primary entry refers to the statement summary section.
- The secondary entry, *usage guidelines*, refers to the section in a configuration guidelines chapter that describes how to use the statement or command.

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xml;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
```

```
        address 10.0.0.1/24;
    }
}
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
  file ex-script-snippet.xml; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see the [Junos OS CLI User Guide](#).

Documentation Conventions

Table 1 on page xxxix 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 xxxix defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: <code>user@host> configure</code>
Fixed-width text like this	Represents output that appears on the terminal screen.	<code>user@host> show chassis alarms</code> <code>No alarms currently active</code>
<i>Italic text like this</i>	<ul style="list-style-type: none"> Introduces important new terms. Identifies book names. Identifies RFC and Internet draft titles. 	<ul style="list-style-type: none"> A policy <i>term</i> is a named structure that defines match conditions and actions. <i>Junos OS System Basics Configuration Guide</i> RFC 1997, <i>BGP Communities Attribute</i>
<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; interface names; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none"> To configure a stub area, include the stub statement at the <code>[edit protocols ospf area area-id]</code> hierarchy level. The console port is labeled CONSOLE.
< > (angle brackets)	Enclose optional keywords or variables.	<code>stub <default-metric <i>metric</i>>;</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.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Enclose a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identify a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none"> In the Logical Interfaces box, select All Interfaces. To cancel the configuration, click Cancel.
> (bold right angle bracket)	Separates levels in a hierarchy of J-Web selections.	In the configuration editor hierarchy, select Protocols>Ospf .

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, 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](#)
- [Network Architecture on page 37](#)

CHAPTER 1

System Architecture

- [Overview of Broadband Gateway System Architecture on page 4](#)
- [Overview of Broadband Gateway System Control Packet Flow on page 6](#)
- [Overview of Broadband Gateway Uplink Payload Packet Flow on page 7](#)
- [Overview of Broadband Gateway Downlink Payload Packet Flow on page 9](#)
- [Overview of Broadband Gateway as GGSN or P-GW on page 10](#)
- [Understanding Mobile User Types on page 11](#)
- [Configuring Broadband Gateway Home PLMNs and Gateways on page 11](#)
- [Configuring Broadband Gateway Local Policies Application on page 12](#)
- [Configuring Broadband Gateway Call Rate Statistics on page 13](#)
- [Verifying the Gateway Configuration on page 14](#)
- [Configuring General Gateway Trace Options on page 15](#)
- [Configuring Mobile Options Trace Options on page 17](#)
- [Configuring Resource Manager Trace Options on page 19](#)
- [Serving Gateways and the MobileNext Broadband Gateway Overview on page 21](#)
- [Overview of Standalone S-GW User Plane Packet Flow on page 25](#)
- [MobileNext Broadband Gateway Configuration Overview on page 26](#)
- [Overview of Collocated Gateways: Control Plane on page 28](#)
- [Overview of Collocated Gateways: User Plane on page 29](#)
- [Configuring an S-GW on a Broadband Gateway on page 30](#)
- [Configuring S-GW-Specific Profiles on page 32](#)
- [Configuring S-GW Traceoptions on page 33](#)

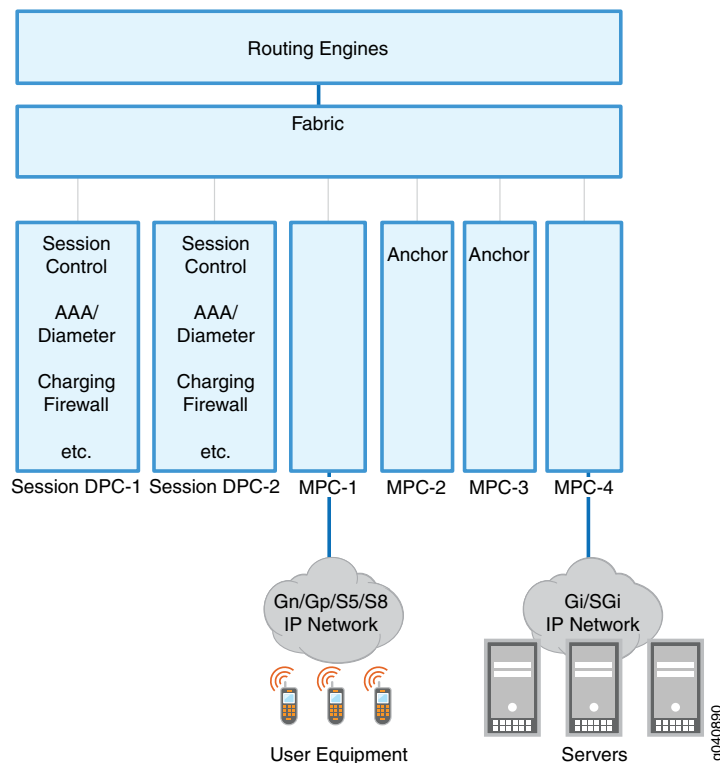
Overview of Broadband Gateway System Architecture

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 6](#)
- [Overview of Broadband Gateway Uplink Payload Packet Flow on page 7](#)
- [Overview of Broadband Gateway Downlink Payload Packet Flow on page 9](#)
- [Overview of Broadband Gateway as GGSN or P-GW on page 10](#)

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

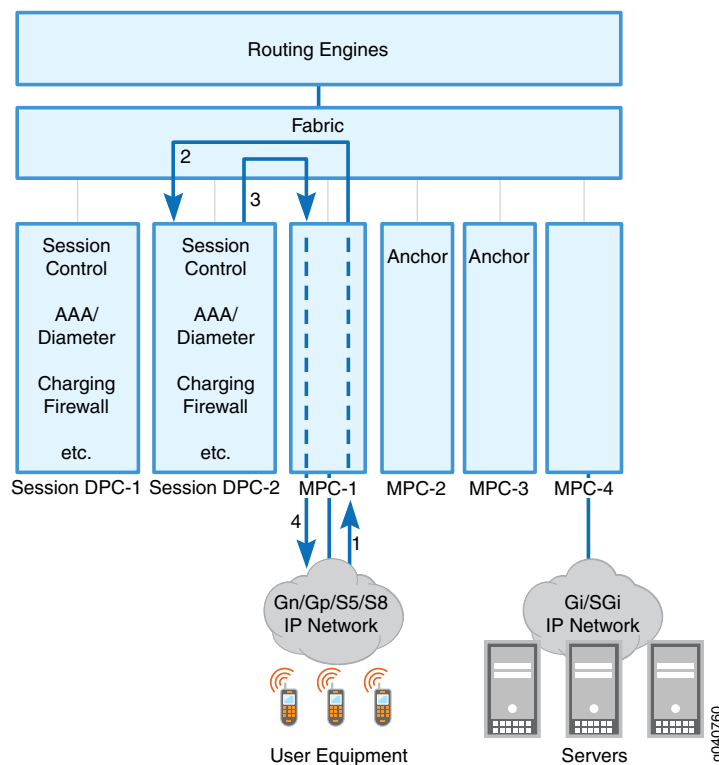


Figure 2 on page 6 shows the four steps that GTP-C signaling packets take through the broadband gateway:

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.

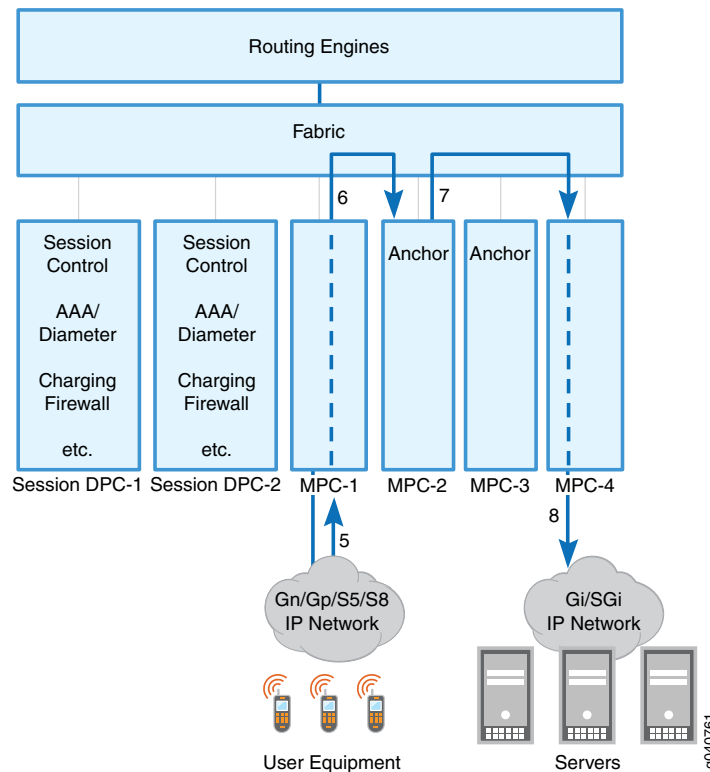
Related Documentation

- [Overview of Broadband Gateway System Architecture on page 4](#)
- [Overview of Broadband Gateway Uplink Payload Packet Flow on page 7](#)
- [Overview of Broadband Gateway Downlink Payload Packet Flow on page 9](#)
- [Overview of Broadband Gateway as GGSN or P-GW on page 10](#)

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.

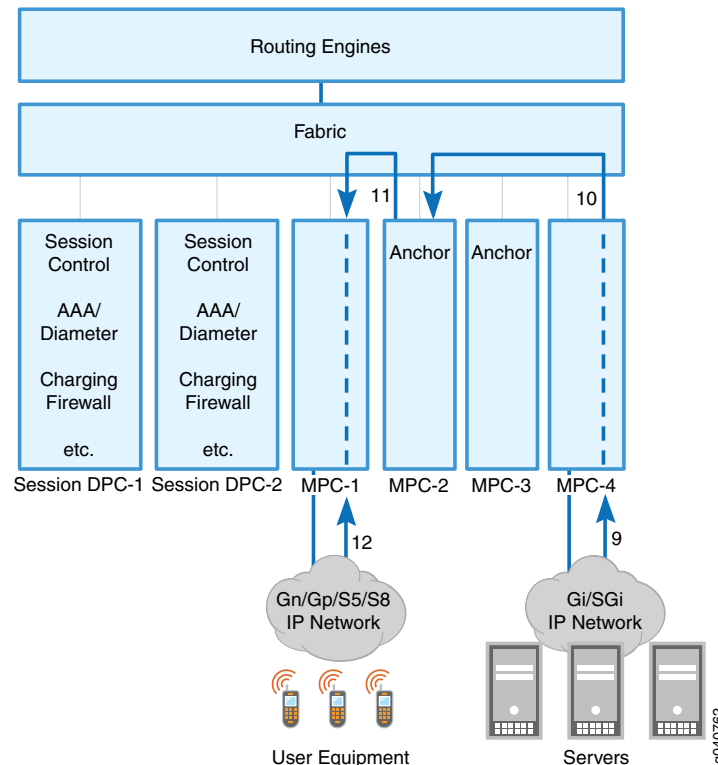
**Related
Documentation**

- [Overview of Broadband Gateway System Architecture on page 4](#)
- [Overview of Broadband Gateway System Control Packet Flow on page 6](#)
- [Overview of Broadband Gateway Downlink Payload Packet Flow on page 9](#)
- [Overview of Broadband Gateway as GGSN or P-GW on page 10](#)

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 9](#) 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 4](#)
- [Overview of Broadband Gateway System Control Packet Flow on page 6](#)
- [Overview of Broadband Gateway Uplink Payload Packet Flow on page 7](#)
- [Overview of Broadband Gateway as GGSN or P-GW on page 10](#)

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 4](#)
- [Configuring Broadband Gateway Home PLMNs and Gateways on page 11](#)

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 SSGN 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 4](#)
- [Configuring Broadband Gateway Home PLMNs and Gateways on page 11](#)
- [Configuring Broadband Gateway Local Policies Application on page 12](#)

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 11](#)
- [Configuring Broadband Gateway Local Policies Application on page 12](#)
- [Overview of Broadband Gateway System Architecture on page 4](#)
- [Configuring General Gateway Trace Options on page 15](#)
- [Configuring Mobile Options Trace Options on page 17](#)
- [Configuring Resource Manager Trace Options on page 19](#)

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 11](#)
- [Overview of Broadband Gateway System Architecture on page 4](#)
- [Configuring General Gateway Trace Options on page 15](#)
- [Configuring Mobile Options Trace Options on page 17](#)
- [Configuring Resource Manager Trace Options on page 19](#)

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 11](#)
- [Configuring General Gateway Trace Options on page 15](#)
- [Configuring Mobile Options Trace Options on page 17](#)
- [Configuring Resource Manager Trace Options on page 19](#)

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 load-info
```

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

```
user@host> show unified-edge ggsn-pgw resource-manger imsi-location-database
```

**Related
Documentation**

- [Configuring Broadband Gateway Home PLMNs and Gateways on page 11](#)
- [Configuring Broadband Gateway Local Policies Application on page 12](#)
- [Configuring Broadband Gateway Call Rate Statistics on page 13](#)

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 15](#) 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
all	Trace everything.
bulkjob	Trace resources.
config	Trace configuration events.
cos-cac	Trace CoS and CAC events.
ctxt	Trace user equipment, PDN, or bearer context events.
fsm	Trace FSM events.
gtpu	Trace GTP-U events.
ha	Trace high availability events.
init	Trace events related to protocol daemon initialization.
pfem	Trace PFE manager events.
stats	Trace stats events.
waitq	Trace waitq events.

[Table 4 on page 15](#) describes the levels you can include.

Table 4: Trace Levels

Level	Description
all	Match all levels.
error	Match error conditions.
info	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 4](#)
- [Configuring Broadband Gateway Home PLMNs and Gateways on page 11](#)
- [Configuring Broadband Gateway Local Policies Application on page 12](#)
- [Configuring Mobile Options Trace Options on page 17](#)

- [Configuring Resource Manager Trace Options on page 19](#)

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 and levels.

[Table 5 on page 17](#) 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
all	Trace everything.
configuration	Trace configuration events.
error	Trace events related to catastrophic errors in the daemon.
init	Trace events related to protocol daemon initialization.
protocol	Trace protocol processing events.

[Table 6 on page 17](#) describes the levels you can include.

Table 6: Trace Levels

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

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. Configure the tracing level.

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

6. View the trace file.

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

**Related
Documentation**

- [Overview of Broadband Gateway System Architecture on page 4](#)
- [Configuring Broadband Gateway Home PLMNs and Gateways on page 11](#)
- [Configuring Broadband Gateway Local Policies Application on page 12](#)
- [Configuring General Gateway Trace Options on page 15](#)
- [Configuring Resource Manager Trace Options on page 19](#)

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 7 on page 19 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 7: Resource Management Server Trace Flags

Flag	Description
all	Trace everything.
communication	Trace Infra code.
config	Trace configuration code.
gres	Trace GRES code.
info-manager	Trace information management code.
init	Trace events related to data path daemon initialization.
memory	Trace memory management code.
packet-steering	Trace packet-steering code.
resource-manager	Trace resource management code.
signal	Trace signal handling code.
state	Trace state handling code.
timer	Trace timer code.
ui	Trace user interface code.

Table 8 on page 20 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 8: Resource Management Client Trace Flags

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

Table 9 on page 20 describes the levels you can include.

Table 9: Trace Levels

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

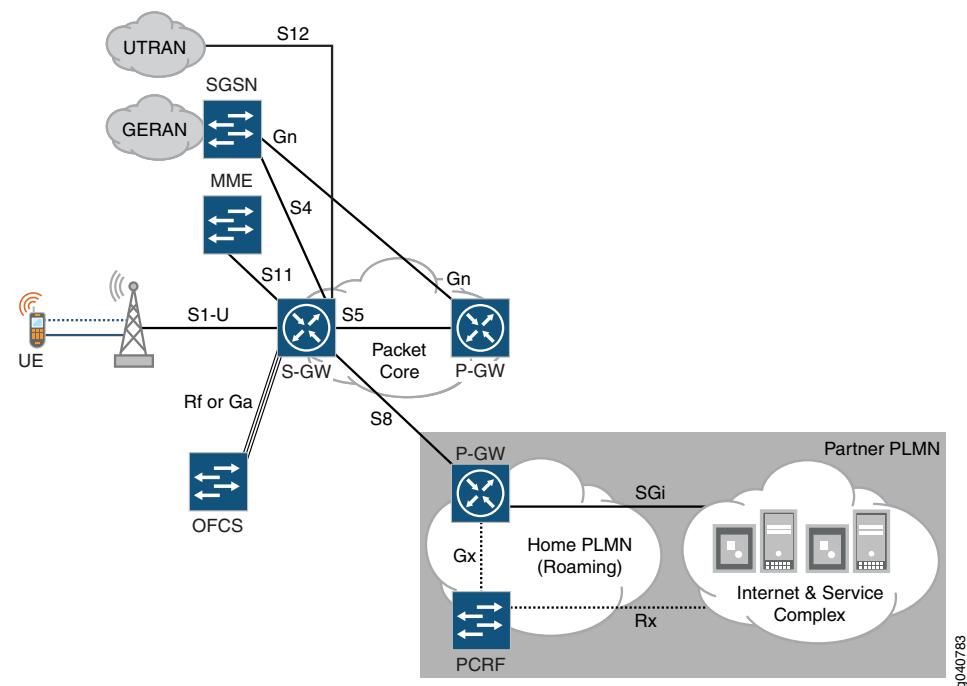
- [Overview of Broadband Gateway System Architecture on page 4](#)
- [Configuring Broadband Gateway Home PLMNs and Gateways on page 11](#)
- [Configuring Broadband Gateway Local Policies Application on page 12](#)
- [Configuring General Gateway Trace Options on page 15](#)
- [Configuring Mobile Options Trace Options on page 17](#)

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 5 on page 22](#).

Figure 5: S-GW Interfaces on the Broadband Gateway



When the broadband gateway is configured as an S-GW, these S-GW functions include:

- Control interfaces between S-GW and SGSN (S4 interface), S-GW and P-GW (S5) and S-GW and Mobility Management Entity (MME) (S11)
- Data interfaces between S-GW and eNodeB (S1-U interface), S-GW and SGSN (S4), S-GW and P-GW, local and roaming (S5/S8), and RNC (S12)
- Support for S-GW Charging Data Records (CDRs)
- Idle mode signaling reduction
- Support for 2G and 3G access



NOTE: There is no support for the S101, S103, or GXc interfaces on the broadband gateway.

A key function of the broadband gateway S-GW is buffering and idle mode handling. When a downlink packet for an idle user device arrives, the S-GW buffers the packet and initiates paging toward to MME/SGSN on the S11 or S4 interface. When the user device moves to active mode, the packet is delivered.

Also, the broadband gateway S-GW uses indirect data forwarding during handover to make sure that uplink or downlink data is not dropped. The S-GW forwards the data and an end marker through indirect data tunnels, and sends end marker packets to ensure in-order data delivery.

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.

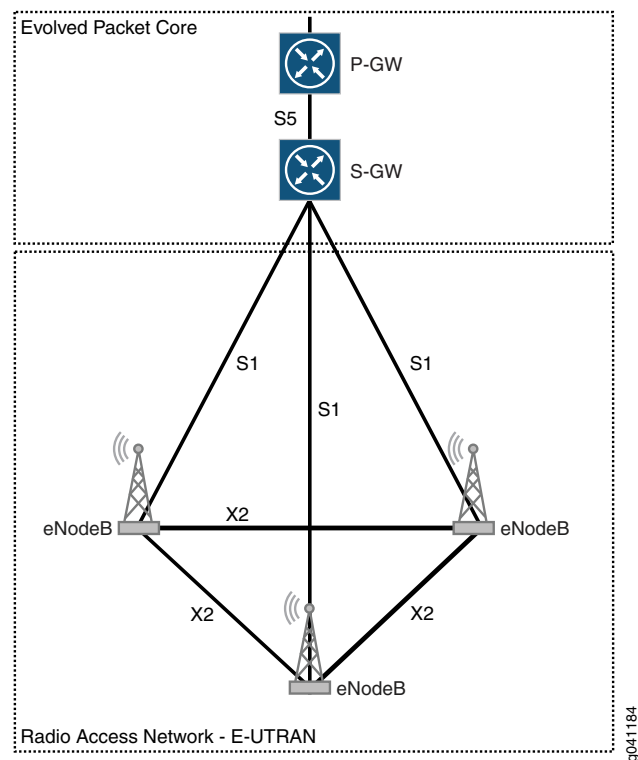
The S1 control plane runs between an eNodeB and a Mobility Management Entity (MME) and is called the S1-MME. Do not confuse the S1-MME (eNodeB-MME interface) with the S11 (S-GW-MME) interface, which carries GPRS tunneling protocol control (GTP-C) messages. On the other hand, the S1 user plane runs between 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 6 on page 24](#) shows the relationship between the S1 and X2 interfaces.

Figure 6: S-GW and the S1 and X2 Interfaces



Related Documentation

- [Overview of Broadband Gateway System Architecture on page 4](#)
- [Overview of Standalone S-GW User Plane Packet Flow on page 25](#)
- [Overview of Collocated Gateways: Control Plane on page 28](#)
- [Overview of Collocated Gateways: User Plane on page 29](#)
- [MobileNext Broadband Gateway Configuration Overview on page 26](#)
- [Configuring an S-GW on a Broadband Gateway on page 30](#)
- [Configuring S-GW-Specific Profiles on page 32](#)
- [Configuring S-GW Traceoptions on page 33](#)

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 7: GTP-U Packet Flow Through Standalone S-GW

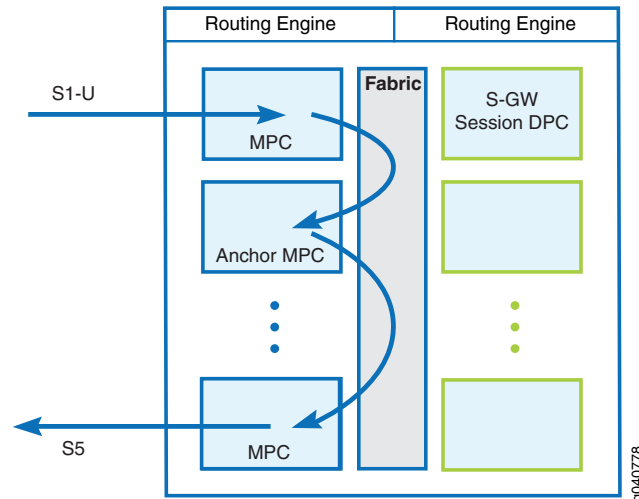


Figure 7 on page 25 shows the usual path of user packets (GTP-U) from eNodeB radio network (S1-U) to P-GW (S5) interfaces. Note that the user packet passes through the S-GW anchor Modular Port Concentrator (MPC) for that particular bearer. They do not flow through a service Packet Forwarding Engine unless 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 4](#)
- [Serving Gateways and the MobileNext Broadband Gateway Overview on page 21](#)
- [Overview of Collocated Gateways: Control Plane on page 28](#)
- [Overview of Collocated Gateways: User Plane on page 29](#)
- [MobileNext Broadband Gateway Configuration Overview on page 26](#)
- [Configuring an S-GW on a Broadband Gateway on page 30](#)
- [Configuring S-GW-Specific Profiles on page 32](#)
- [Configuring S-GW Traceoptions on page 33](#)

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 8: Collocated Gateways S-GW and P-GW Resources and Load Balancing

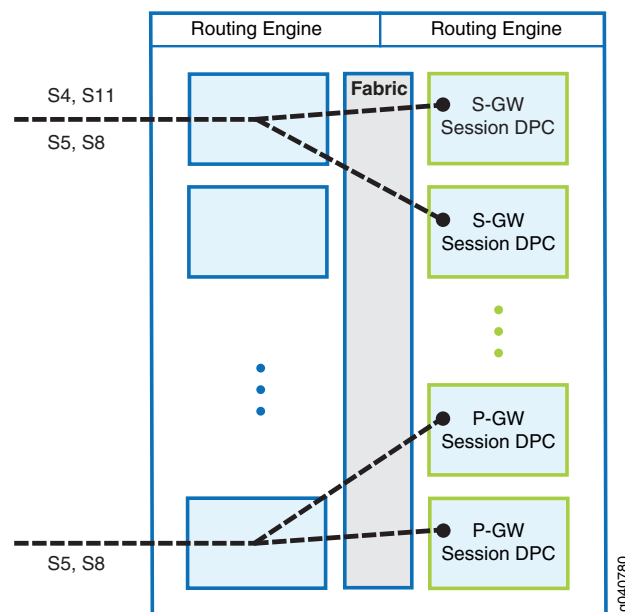


Figure 8 on page 26 shows how resource sharing and load balancing takes place in a collocated S-GW and P-GW configured on the broadband gateway. No matter how the broadband gateway is utilized, the chassis configuration for Modular Port Concentrators (MPCs), Dense Port Concentrators (DPCs), anchors, 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 4](#)
- [Serving Gateways and the MobileNext Broadband Gateway Overview on page 21](#)
- [Overview of Collocated Gateways: Control Plane on page 28](#)
- [Overview of Collocated Gateways: User Plane on page 29](#)
- [Configuring an S-GW on a Broadband Gateway on page 30](#)
- [Configuring S-GW-Specific Profiles on page 32](#)
- [Configuring S-GW Traceoptions on page 33](#)

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 9: Collocated S-GW and P-GW Control Packet Flow

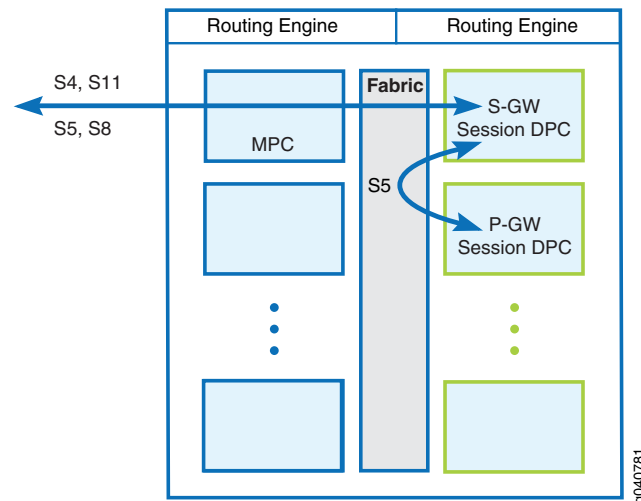


Figure 9 on page 28 shows the path of GTP-C packets through the broadband gateway when configured as a collocated S-GW and P-GW.

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 4](#)
- [Serving Gateways and the MobileNext Broadband Gateway Overview on page 21](#)
- [Overview of Standalone S-GW User Plane Packet Flow on page 25](#)
- [Overview of Collocated Gateways: User Plane on page 29](#)

- [Configuring an S-GW on a Broadband Gateway on page 30](#)
- [Configuring S-GW-Specific Profiles on page 32](#)
- [Configuring S-GW Traceoptions on page 33](#)

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 10: Collocated S-GW and P-GW User Packet Flow

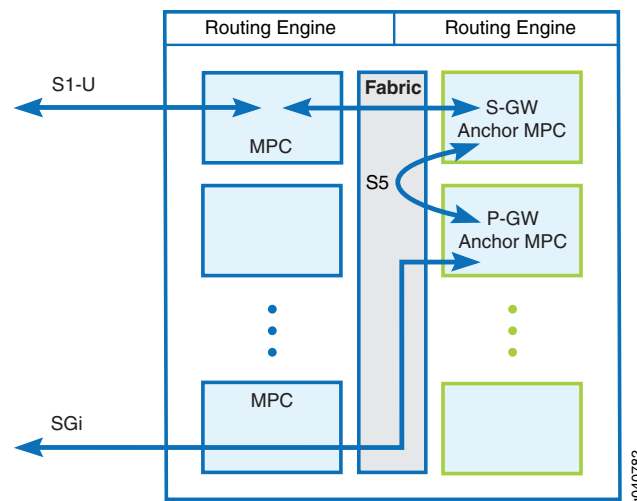


Figure 10 on page 29 shows a collocated P-GW and S-GW in the same broadband gateway. The usual path of user packets from eNodeB radio network (S1-U) to internal S5 interface to SGi interface is shown. Note that the user packet passes through the S-GW and P-GW anchor Modular Port Concentrators (MPCs) 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 4](#)
- [Serving Gateways and the MobileNext Broadband Gateway Overview on page 21](#)
- [Overview of Standalone S-GW User Plane Packet Flow on page 25](#)
- [Overview of Collocated Gateways: Control Plane on page 28](#)
- [Configuring an S-GW on a Broadband Gateway on page 30](#)
- [Configuring S-GW-Specific Profiles on page 32](#)
- [Configuring S-GW Traceoptions on page 33](#)

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 4](#)
- [Serving Gateways and the MobileNext Broadband Gateway Overview on page 21](#)
- [Overview of Standalone S-GW User Plane Packet Flow on page 25](#)

- [Overview of Collocated Gateways: Control Plane on page 28](#)
- [Overview of Collocated Gateways: User Plane on page 29](#)
- [Configuring S-GW-Specific Profiles on page 32](#)
- [Configuring S-GW Traceoptions on page 33](#)

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 configure 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 4](#)
- [Serving Gateways and the MobileNext Broadband Gateway Overview on page 21](#)
- [Overview of Standalone S-GW User Plane Packet Flow on page 25](#)

- [Overview of Collocated Gateways: Control Plane on page 28](#)
- [Overview of Collocated Gateways: User Plane on page 29](#)
- [Configuring an S-GW on a Broadband Gateway on page 30](#)
- [Configuring S-GW Traceoptions on page 33](#)

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 10 on page 33](#) 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 10: 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.
ctxt	Trace user equipment, packet data network, and bearer context events.
fsm	Trace finite state machine events.
gtpu	Trace GPRS tunneling protocol, user (GTP-U) protocol events.
ha	Trace high availability events.
init	Trace initialization events.
pfem	Trace Packet Forwarding Engine manager events.
stats	Trace statistic events.
waitq	Trace wait queue events.

[Table 11 on page 33](#) describes the levels you can include.

Table 11: S-GW Trace Levels

Level	Description
-------	-------------

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

all	Match all levels.
error	Match error conditions.
info	Match informational messages.
notice	Match conditions that should be specially handled.
verbose	Match verbose messages.
warning	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 4](#)
- [Serving Gateways and the MobileNext Broadband Gateway Overview on page 21](#)
- [Overview of Standalone S-GW User Plane Packet Flow on page 25](#)
- [Overview of Collocated Gateways: Control Plane on page 28](#)
- [Overview of Collocated Gateways: User Plane on page 29](#)
- [Configuring an S-GW on a Broadband Gateway on page 30](#)
- [Configuring S-GW-Specific Profiles on page 32](#)
- [Configuring S-GW Data Path Traceoptions on page 97](#)
- [Configuring S-GW GTP Traceoptions on page 262](#)
- [Configuring S-GW Charging Traceoptions on page 284](#)
- [Configuring S-GW Local Persistent Storage Traceoptions on page 287](#)

CHAPTER 2

Network Architecture

- [Overview of Mobile Networks on page 37](#)
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 39](#)
- [Overview of GGSN and P-GW on page 40](#)
- [Overview of Packet Data Network Gateway Functions on page 42](#)
- [Overview of the Evolved Packet Core on page 44](#)
- [Overview of APNs on page 46](#)
- [Overview of PDP Contexts and Bearers on page 47](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 49](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 50](#)
- [Overview of IPv6 and the Broadband Gateway on page 52](#)
- [Serving Gateway and the S1 Interface Overview on page 53](#)
- [Service Areas and Tracking Areas Overview on page 54](#)
- [Serving Gateway Functions Overview on page 55](#)

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**

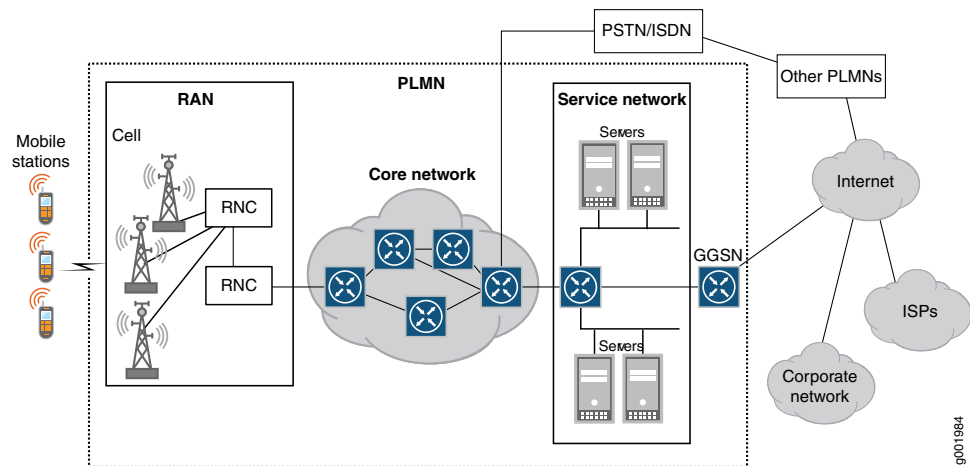
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 39](#)
- [Overview of GGSN and P-GW on page 40](#)
- [Overview of Packet Data Network Gateway Functions on page 42](#)
- [Overview of the Evolved Packet Core on page 44](#)
- [Overview of APNs on page 46](#)
- [Overview of PDP Contexts and Bearers on page 47](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 49](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 50](#)
- [Overview of IPv6 and the Broadband Gateway on page 52](#)
- [Overview of IPv6 and the Broadband Gateway on page 52](#)
- [Serving Gateway and the S1 Interface Overview on page 53](#)
- [Serving Gateway and the S1 Interface Overview on page 53](#)
- [Service Areas and Tracking Areas Overview on page 54](#)

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 11 on page 39 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 11: 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 11 on page 39. 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 11 on page 39) 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**

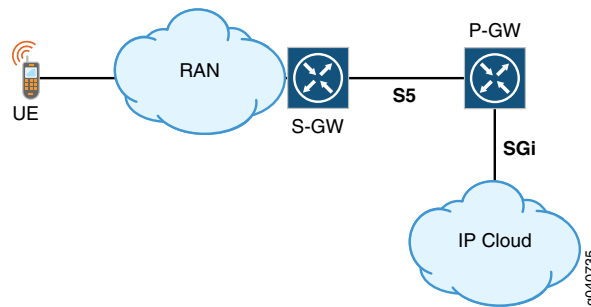
- [Overview of Mobile Networks on page 37](#)
- [Overview of GGSN and P-GW on page 40](#)
- [Overview of Packet Data Network Gateway Functions on page 42](#)
- [Overview of the Evolved Packet Core on page 44](#)
- [Overview of APNs on page 46](#)
- [Overview of PDP Contexts and Bearers on page 47](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 49](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 50](#)
- [Overview of IPv6 and the Broadband Gateway on page 52](#)
- [Overview of IPv6 and the Broadband Gateway on page 52](#)
- [Serving Gateway and the S1 Interface Overview on page 53](#)
- [Serving Gateway and the S1 Interface Overview on page 53](#)
- [Service Areas and Tracking Areas Overview on page 54](#)

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 12 on page 41](#) shows the major components and interfaces of a mobile network based on 4G/LTE standards.

Figure 12: 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 37](#)
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 39](#)
- [Overview of Packet Data Network Gateway Functions on page 42](#)
- [Overview of the Evolved Packet Core on page 44](#)
- [Overview of APNs on page 46](#)
- [Overview of PDP Contexts and Bearers on page 47](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 49](#)

- [Overview of 4G/LTE and Broadband Gateway Deployment on page 50](#)
- [Overview of IPv6 and the Broadband Gateway on page 52](#)
- [Overview of IPv6 and the Broadband Gateway on page 52](#)
- [Serving Gateway and the S1 Interface Overview on page 53](#)
- [Serving Gateway and the S1 Interface Overview on page 53](#)
- [Service Areas and Tracking Areas Overview on page 54](#)

Overview of Packet Data Network Gateway Functions

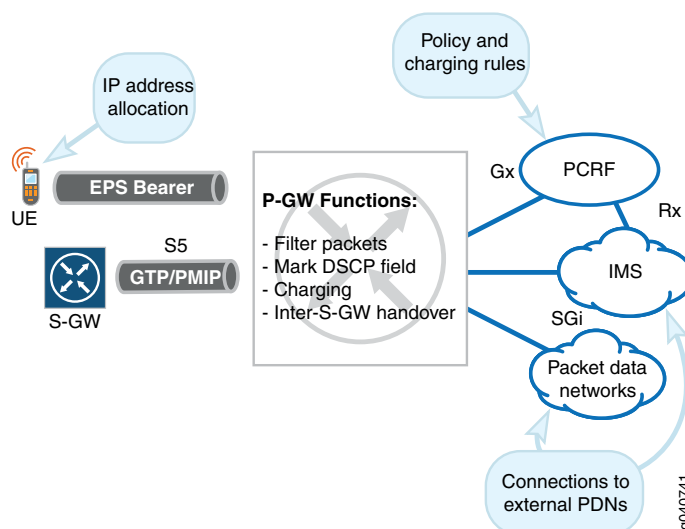
In a mobile network, a major function of the Packet Data Network Gateway (P-GW) is to allocate IP addresses to the user equipment during default bearer setup. The user equipment can still connect to multiple packet networks through multiple P-GWs, and also to older, non-3GPP-compliant IP networks.



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 13: 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 13 on page 42](#) 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

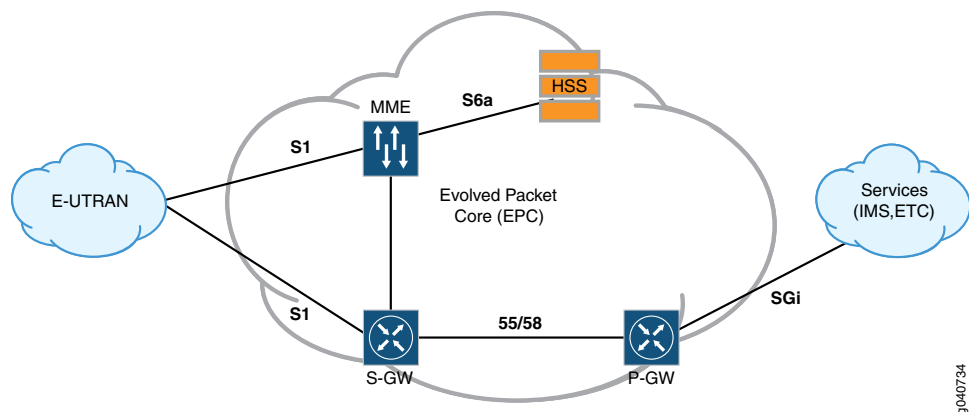
- [Overview of Mobile Networks on page 37](#)
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 39](#)
- [Overview of GGSN and P-GW on page 40](#)
- [Overview of the Evolved Packet Core on page 44](#)
- [Overview of APNs on page 46](#)
- [Overview of PDP Contexts and Bearers on page 47](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 49](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 50](#)
- [Overview of IPv6 and the Broadband Gateway on page 52](#)
- [Overview of IPv6 and the Broadband Gateway on page 52](#)
- [Serving Gateway and the S1 Interface Overview on page 53](#)
- [Serving Gateway and the S1 Interface Overview on page 53](#)
- [Service Areas and Tracking Areas Overview on page 54](#)

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 14 on page 44 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 14: 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**

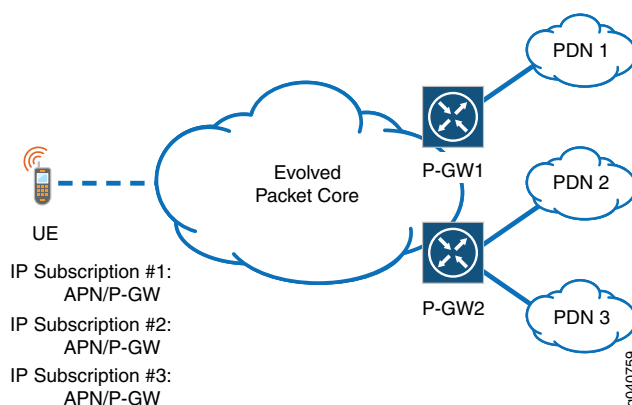
- [Overview of Mobile Networks on page 37](#)
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 39](#)
- [Overview of GGSN and P-GW on page 40](#)
- [Overview of Packet Data Network Gateway Functions on page 42](#)
- [Overview of APNs on page 46](#)
- [Overview of PDP Contexts and Bearers on page 47](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 49](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 50](#)
- [Overview of IPv6 and the Broadband Gateway on page 52](#)
- [Overview of IPv6 and the Broadband Gateway on page 52](#)
- [Serving Gateway and the S1 Interface Overview on page 53](#)
- [Serving Gateway and the S1 Interface Overview on page 53](#)
- [Service Areas and Tracking Areas Overview on page 54](#)

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 15 on page 46](#) shows the relationship among APNs, P-GWs, and packet networks.

Figure 15: 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**

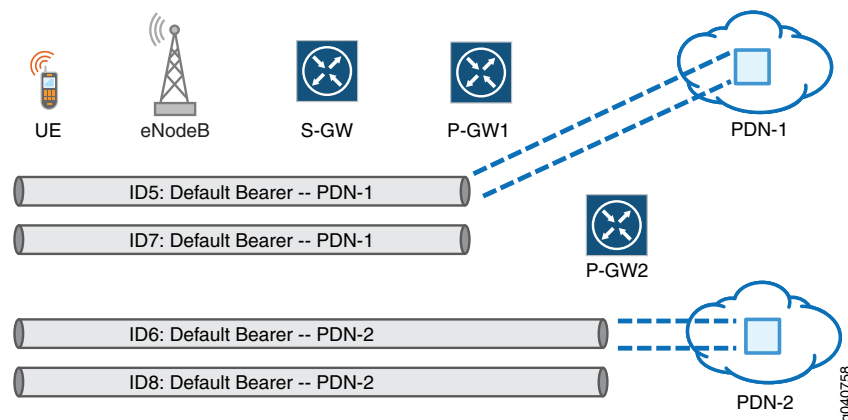
- [Overview of Mobile Networks on page 37](#)
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 39](#)
- [Overview of GGSN and P-GW on page 40](#)
- [Overview of Packet Data Network Gateway Functions on page 42](#)
- [Overview of the Evolved Packet Core on page 44](#)
- [Overview of PDP Contexts and Bearers on page 47](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 49](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 50](#)
- [Overview of IPv6 and the Broadband Gateway on page 52](#)
- [Overview of IPv6 and the Broadband Gateway on page 52](#)
- [Serving Gateway and the S1 Interface Overview on page 53](#)
- [Serving Gateway and the S1 Interface Overview on page 53](#)
- [Service Areas and Tracking Areas Overview on page 54](#)

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 16 on page 48](#) shows the relationship between bearers and P-GWs.

Figure 16: 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

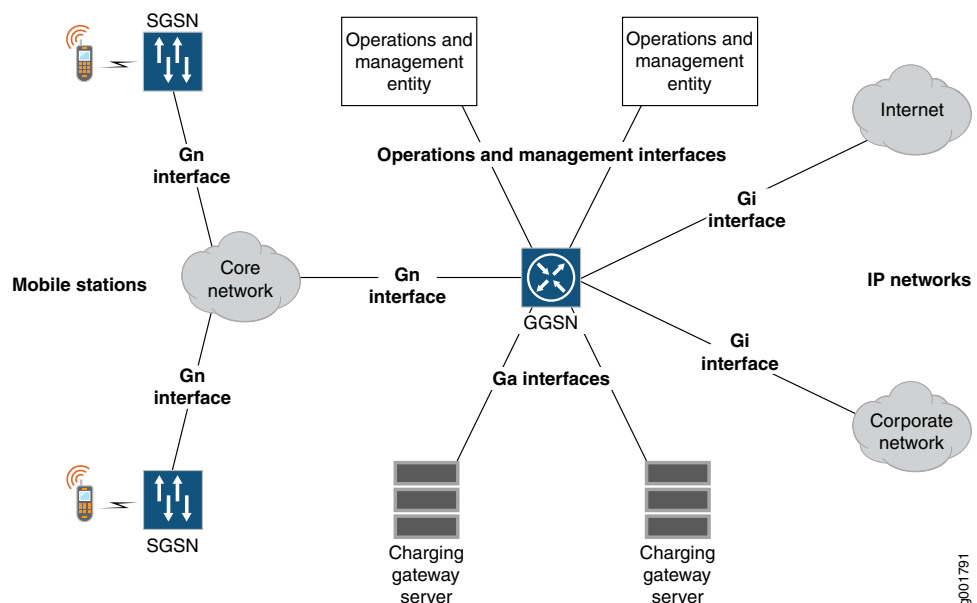
- [Overview of Mobile Networks on page 37](#)
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 39](#)
- [Overview of GGSN and P-GW on page 40](#)
- [Overview of Packet Data Network Gateway Functions on page 42](#)
- [Overview of the Evolved Packet Core on page 44](#)
- [Overview of APNs on page 46](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 49](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 50](#)
- [Overview of IPv6 and the Broadband Gateway on page 52](#)
- [Overview of IPv6 and the Broadband Gateway on page 52](#)
- [Serving Gateway and the S1 Interface Overview on page 53](#)
- [Serving Gateway and the S1 Interface Overview on page 53](#)
- [Service Areas and Tracking Areas Overview on page 54](#)

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 17 on page 49](#) 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 17: 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**

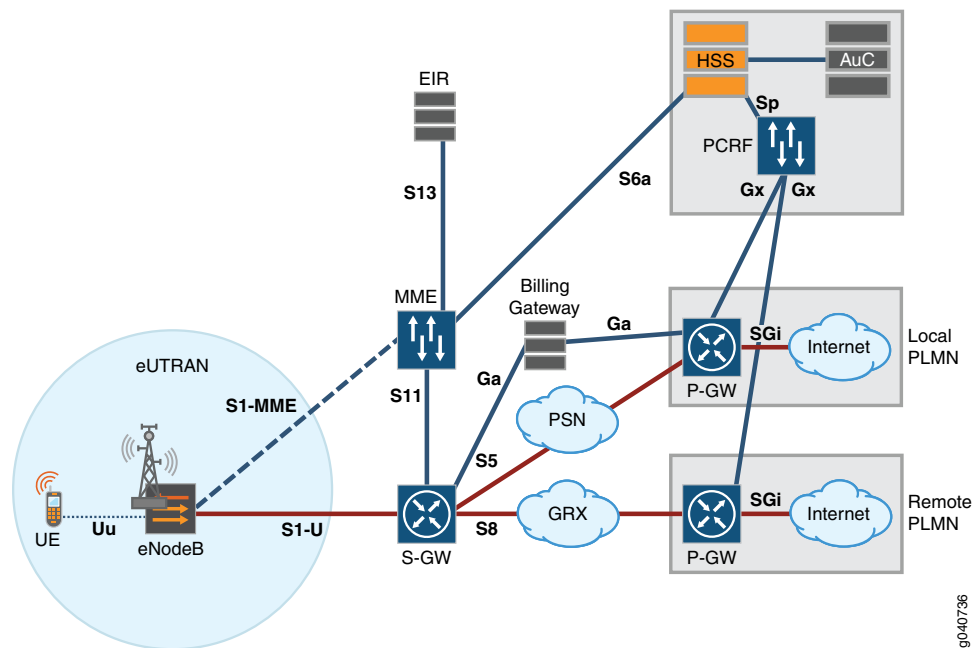
- [Overview of Mobile Networks on page 37](#)
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 39](#)
- [Overview of GGSN and P-GW on page 40](#)
- [Overview of Packet Data Network Gateway Functions on page 42](#)
- [Overview of the Evolved Packet Core on page 44](#)
- [Overview of APNs on page 46](#)
- [Overview of PDP Contexts and Bearers on page 47](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 50](#)
- [Overview of IPv6 and the Broadband Gateway on page 52](#)
- [Overview of IPv6 and the Broadband Gateway on page 52](#)
- [Serving Gateway and the S1 Interface Overview on page 53](#)
- [Serving Gateway and the S1 Interface Overview on page 53](#)
- [Service Areas and Tracking Areas Overview on page 54](#)

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 18 on page 51](#) 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 18: 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 37](#)
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 39](#)
- [Overview of GGSN and P-GW on page 40](#)
- [Overview of Packet Data Network Gateway Functions on page 42](#)
- [Overview of the Evolved Packet Core on page 44](#)
- [Overview of APNs on page 46](#)
- [Overview of PDP Contexts and Bearers on page 47](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 49](#)
- [Overview of IPv6 and the Broadband Gateway on page 52](#)
- [Serving Gateway and the S1 Interface Overview on page 53](#)
- [Serving Gateway and the S1 Interface Overview on page 53](#)
- [Service Areas and Tracking Areas Overview on page 54](#)

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 37](#)
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 39](#)
- [Overview of GGSN and P-GW on page 40](#)
- [Overview of Packet Data Network Gateway Functions on page 42](#)
- [Overview of the Evolved Packet Core on page 44](#)

- [Overview of APNs on page 46](#)
- [Overview of PDP Contexts and Bearers on page 47](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 49](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 50](#)
- [Serving Gateway and the S1 Interface Overview on page 53](#)
- [Serving Gateway and the S1 Interface Overview on page 53](#)
- [Service Areas and Tracking Areas Overview on page 54](#)

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 19: S1 Interface Is Many-to-Many

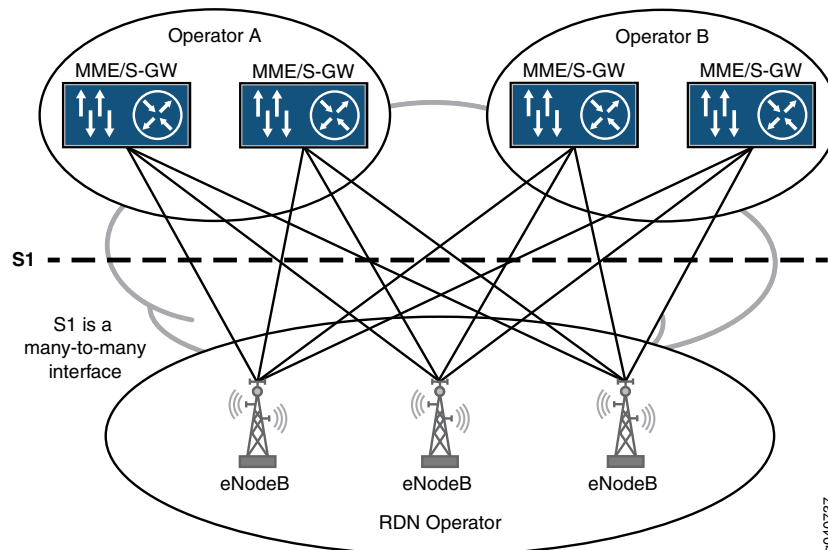


Figure 19 on page 53 shows that the S1 interface between eNodeBs and the MMEs and S-GWs is a many-to-many interface. The S1 interface supports redundancy and load sharing of these critical network nodes. Load sharing the MMEs allows the user equipment to operate in a given geographical area without changing 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 37](#)
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 39](#)
- [Overview of GGSN and P-GW on page 40](#)

- [Overview of Packet Data Network Gateway Functions on page 42](#)
- [Overview of the Evolved Packet Core on page 44](#)
- [Overview of APNs on page 46](#)
- [Overview of PDP Contexts and Bearers on page 47](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 49](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 50](#)
- [Overview of IPv6 and the Broadband Gateway on page 52](#)
- [Service Areas and Tracking Areas Overview on page 54](#)
- [Serving Gateway Functions Overview on page 55](#)

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 20: Tracking Areas and the S1 Interface

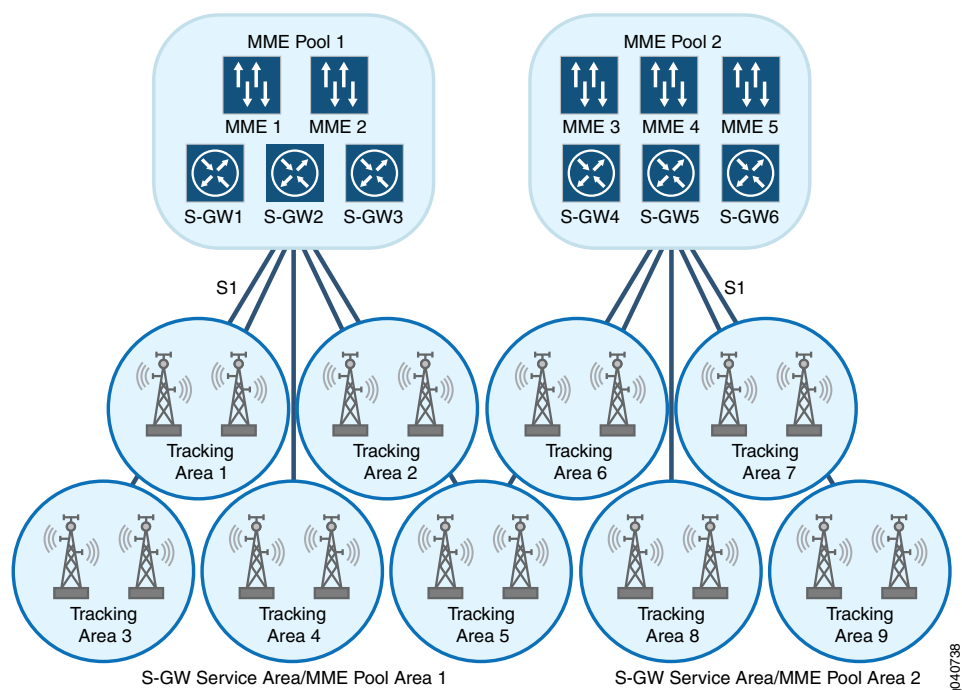


Figure 20 on page 54 shows the relationship between MME pools, S-GW serving areas (which coincide in this case), and enhanced Node B (eNodeB) tracking areas. A mobile user can move around inside the areas of this example network without changing either S-GW or MME. However, if the mobile user moves between 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

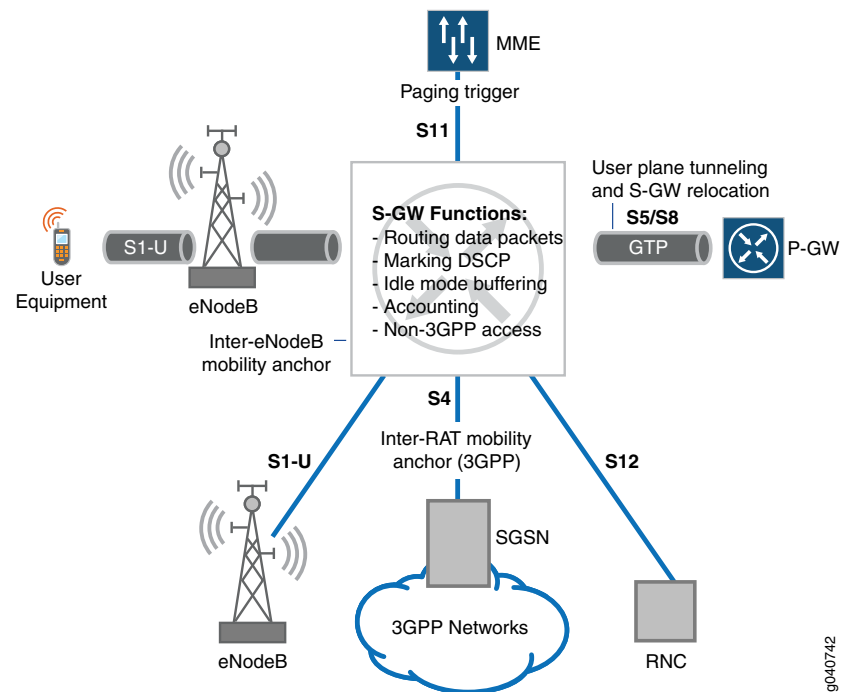
- [Overview of Mobile Networks on page 37](#)
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 39](#)
- [Overview of GGSN and P-GW on page 40](#)
- [Overview of Packet Data Network Gateway Functions on page 42](#)
- [Overview of the Evolved Packet Core on page 44](#)
- [Overview of APNs on page 46](#)
- [Overview of PDP Contexts and Bearers on page 47](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 49](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 50](#)
- [Overview of IPv6 and the Broadband Gateway on page 52](#)
- [Serving Gateway and the S1 Interface Overview on page 53](#)
- [Serving Gateway Functions Overview on page 55](#)

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 21 on page 56 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 21: 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 37
- Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 39
- Overview of GGSN and P-GW on page 40
- Overview of Packet Data Network Gateway Functions on page 42
- Overview of the Evolved Packet Core on page 44
- Overview of APNs on page 46

- [Overview of PDP Contexts and Bearers on page 47](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 49](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 50](#)
- [Overview of IPv6 and the Broadband Gateway on page 52](#)
- [Serving Gateway and the S1 Interface Overview on page 53](#)
- [Service Areas and Tracking Areas Overview on page 54](#)

PART 2

System Configuration

- [Configuring Mobility on MX 3D Devices on page 61](#)
- [Configuring Redundancy on MX 3D Devices on page 73](#)
- [Configuring Mobile Edge Exception Handling on page 87](#)

CHAPTER 3

Configuring Mobility on MX 3D Devices

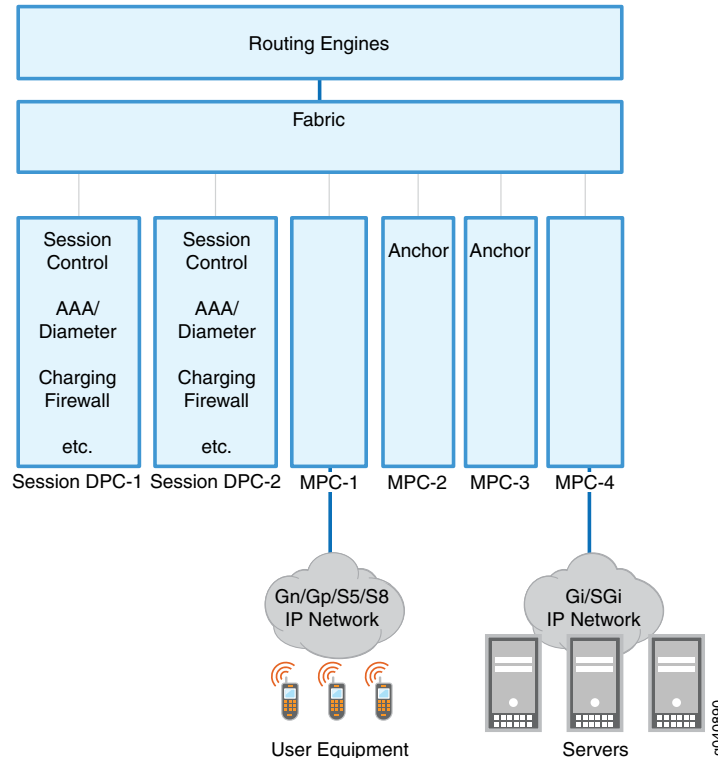
- [MobileNext Broadband Gateway Chassis Overview on page 62](#)
- [Configuring Session DPCs for Mobility on page 64](#)
- [Configuring Interface DPCs or MPCs for User Mobility Traffic on page 66](#)
- [Example: Configuring the MobileNext Broadband Gateway Chassis on page 67](#)
- [Understanding the MobileNext Broadband Gateway Anchors on page 69](#)
- [Configuring Anchor Session DPCs and PFEs on page 71](#)
- [Verifying the MobileNext Broadband Gateway Chassis Configuration on page 72](#)

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 22 on page 62](#), the session DPCs are shown on the left and the interface boards are shown as MPCs on the right.

Figure 22: Session DPCs and Interfaces on the Broadband Gateway



This chassis configuration overview covers:

- [Session DPCs for Mobility on page 63](#)
- [Overview of Mobility Interface Types on page 63](#)

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

- [Example: Configuring the MobileNext Broadband Gateway Chassis on page 67](#)
- [Configuring Session DPCs for Mobility on page 64](#)
- [Configuring Interface DPCs or MPCs for User Mobility Traffic on page 66](#)
- [Understanding the MobileNext Broadband Gateway Anchors on page 69](#)
- [Configuring Anchor Session DPCs and PFEs on page 71](#)
- [Verifying the MobileNext Broadband Gateway Chassis Configuration on page 72](#)

- [Overview of Broadband Gateway System Architecture on page 4](#)

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 62](#)
- [Example: Configuring the MobileNext Broadband Gateway Chassis on page 67](#)
- [Configuring Interface DPCs or MPCs for User Mobility Traffic on page 66](#)
- [Understanding the MobileNext Broadband Gateway Anchors on page 69](#)
- [Configuring Anchor Session DPCs and PFEs on page 71](#)
- [Verifying the MobileNext Broadband Gateway Chassis Configuration on page 72](#)
- [Overview of Broadband Gateway System Architecture on page 4](#)

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 64](#)
- [Configuring Anchor Session DPCs and PFEs on page 71](#)
- [Verifying the MobileNext Broadband Gateway Chassis Configuration on page 72](#)

Example: Configuring the MobileNext Broadband Gateway Chassis

This example shows the configuration of an MX Series router equipped with two session Dense Port Concentrators (DPCs) in FPC slots 1 and 3 and two interface Modular Port Concentrators (MPCs) in FPC slots 0 and 5. The packet network interface **ge-0/0/0.0** is an SGI P-GW 4G/LTE interface and **ge-0/0/0.5** is a 3G GGSN Gi interface. The Gn interfaces are not considered in this example.



NOTE: This is not a functional configuration. Usually, the configuration would include other statements such as access point names (APNs), other interfaces, and so on. This is intended only to illustrate chassis configuration basics.

The following portion of the example shows the chassis slot configuration:

```
[edit chassis]
fpc 0 {    # FPC slot 0 is an interface MPC
  forwarding-packages {
    mobility ggsn-pgw;
  }
}
fpc 1 {    # FPC slot 1 is a Session DPC with 2 PICs
  pic 0 {
    adaptive-services {
      service-package {
```

```
        extension-provider {
            control-cores 1;
            data-cores 2;
            data-flow-affinity;
            data-pollers 1;
            object-cache-size 512;
            total-wired-memory 14336;
            package jservices-mobile;
        }
    }
}
pic 1 {
    adaptive-services {
        service-package {
            extension-provider {
                control-cores 1;
                data-cores 2;
                data-flow-affinity;
                data-pollers 1;
                object-cache-size 512;
                total-wired-memory 14336;
                package jservices-mobile;
            }
        }
    }
}
}
fpc 3 {    # FPC slot 3 is a Session DPC with 2 PICs
    pic 0 {
        adaptive-services {
            service-package {
                extension-provider {
                    control-cores 1;
                    data-cores 2;
                    data-flow-affinity;
                    data-pollers 1;
                    object-cache-size 512;
                    total-wired-memory 14336;
                    package jservices-mobile;
                }
            }
        }
    }
    pic 1 {
        adaptive-services {
            service-package {
                extension-provider {
                    control-cores 1;
                    data-cores 2;
                    data-flow-affinity;
                    data-pollers 1;
                    object-cache-size 512;
                    total-wired-memory 14336;
                    package jservices-mobile;
                }
            }
        }
    }
}
```

```

    }
  }
}
fpc 5 {    # FPC slot 5 is an interface MPC
  forwarding-packages {
    mobility ggsn-pgw;
  }
}

```



NOTE: A complete configuration would include the APNs and other mobility parameters.

Related Documentation

- [Configuring Session DPCs for Mobility on page 64](#)
- [Configuring Interface DPCs or MPCs for User Mobility Traffic on page 66](#)
- [Configuring Anchor Session DPCs and PFEs on page 71](#)
- [Verifying the MobileNext Broadband Gateway Chassis Configuration on page 72](#)

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 23: Upstream GTP-U Traffic

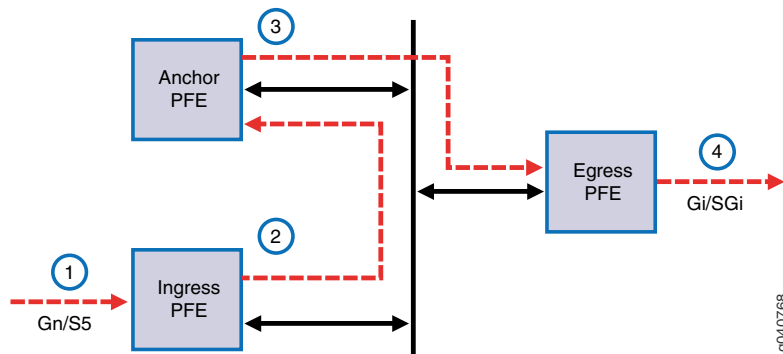


Figure 23 on page 70 shows how all GPRS tunneling protocol, user plane (GTP-U) traffic traverses an anchor Packet Forwarding Engine upstream from a Gn or S5 interface to a Gi or SGi interface:

- 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 24: Downstream GTP-U Traffic

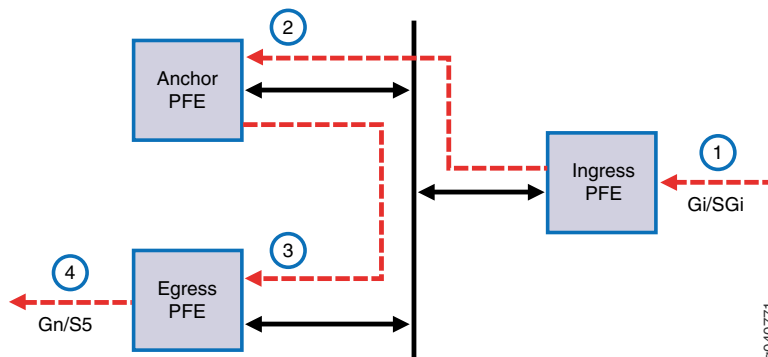


Figure 23 on page 70 shows how all GTP-U traffic traverses an anchor Packet Forwarding Engine downstream from a Gi or SGi interface to a Gn or S5 interface:

- 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 71](#)
- [MobileNext Broadband Gateway Chassis Overview on page 62](#)
- [Configuring Session DPCs for Mobility on page 64](#)
- [Configuring Interface DPCs or MPCs for User Mobility Traffic on page 66](#)
- [Verifying the MobileNext Broadband Gateway Chassis Configuration on page 72](#)

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 64](#)
- [Configuring Interface DPCs or MPCs for User Mobility Traffic on page 66](#)
- [Example: Configuring the MobileNext Broadband Gateway Chassis on page 67](#)
- [Verifying the MobileNext Broadband Gateway Chassis Configuration on page 72](#)

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 64](#)
- [Configuring Interface DPCs or MPCs for User Mobility Traffic on page 66](#)
- [Example: Configuring the MobileNext Broadband Gateway Chassis on page 67](#)
- [Configuring Anchor Session DPCs and PFEs on page 71](#)

CHAPTER 4

Configuring Redundancy on MX 3D Devices

- [Broadband Gateway Redundancy Overview on page 74](#)
- [Configuring Session DPC Redundancy on page 76](#)
- [Configuring Interface Redundancy on page 78](#)
- [Understanding the Broadband Gateway Anchor Failover Behavior on page 80](#)
- [Example: Configuring Broadband Gateway Redundancy on page 82](#)

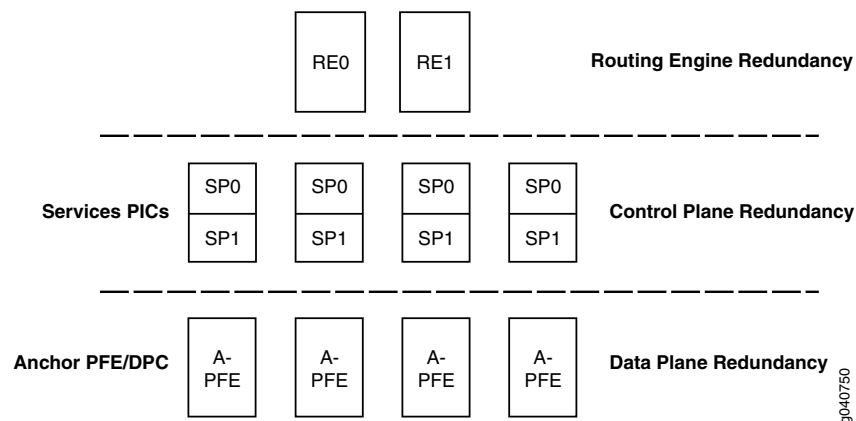
Broadband Gateway Redundancy Overview

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 25 on page 74 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 25: Redundancy Available on the Broadband Gateway



This redundancy configuration overview covers:

- [Routing Engine Redundancy on page 74](#)
- [Session DPC Redundancy on page 75](#)
- [Interface Redundancy on page 76](#)

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 76](#)
- [Configuring Interface Redundancy on page 78](#)
- [Understanding the Broadband Gateway Anchor Failover Behavior on page 80](#)
- [Example: Configuring Broadband Gateway Redundancy on page 82](#)
- [Configuring Anchor Session DPCs and PFEs on page 71](#)

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 74](#)
- [Configuring Interface Redundancy on page 78](#)
- [Understanding the Broadband Gateway Anchor Failover Behavior on page 80](#)
- [Example: Configuring Broadband Gateway Redundancy on page 82](#)
- [Configuring Anchor Session DPCs and PFEs on page 71](#)

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.

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 **apfe0** with all Packet Forwarding Engines in FPC slot 2 and 3 backed up in warm standby by the Packet Forwarding Engines in FPC slot 4.

[edit interfaces]

```
user@host# set apfe0 anchoring-options primary-list fpc-2
user@host# set apfe0 anchoring-options primary-list fpc-3
user@host# set apfe0 anchoring-options secondary fpc-4
user@host# set apfe0 anchoring-options warm-standby
```



NOTE: The warm-standby option is the only mode currently supported. In this configuration (for example) ge-2/0/0 is backed up by ge-4/0/0, ge-2/1/0 is backed up by ge-4/1/0, and so on.

2. Alternatively, 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.

3. 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

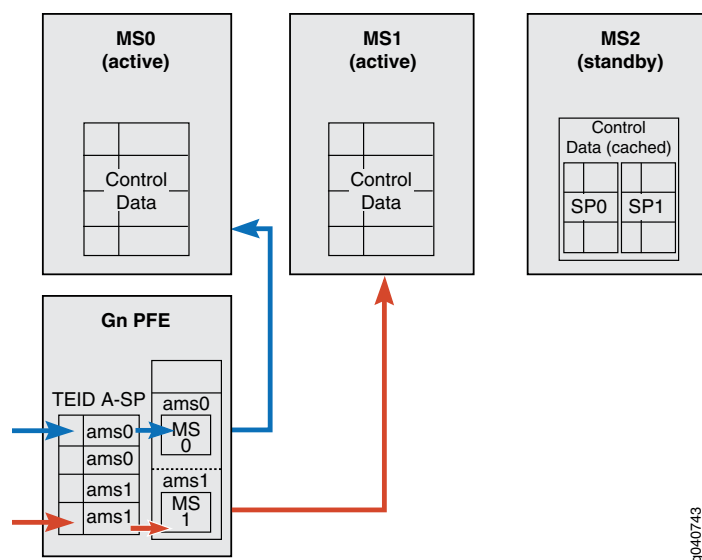
- [Broadband Gateway Redundancy Overview on page 74](#)
- [Configuring Session DPC Redundancy on page 76](#)
- [Understanding the Broadband Gateway Anchor Failover Behavior on page 80](#)

- [Example: Configuring Broadband Gateway Redundancy on page 82](#)
- [Configuring Anchor Session DPCs and PFEs on page 71](#)

Understanding the Broadband Gateway Anchor Failover Behavior

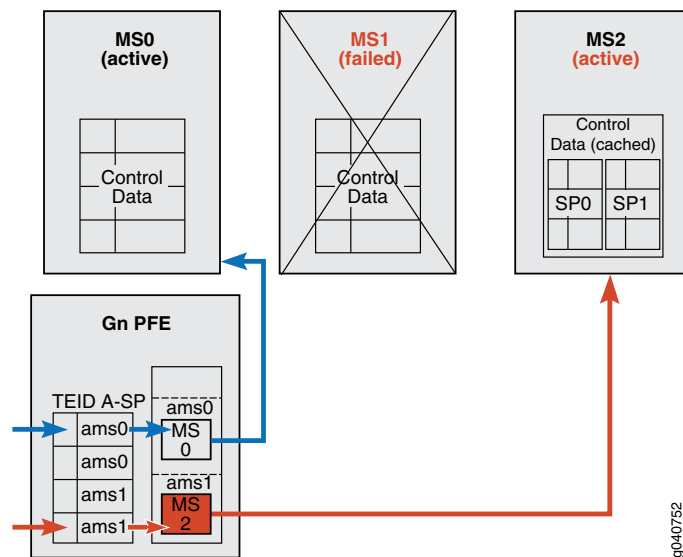
The MobileNext Broadband Gateway anchor session Dense Port Concentrators (DPCs) (housing PICs) and interface PFEs can be configured for redundancy. However, due to the different nature of the redundancy involved, 1:1 for anchor session PICs and N:1 for anchor interface PFEs, the failover behavior is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

Figure 26: Control Plane Anchor Operation Before Failure



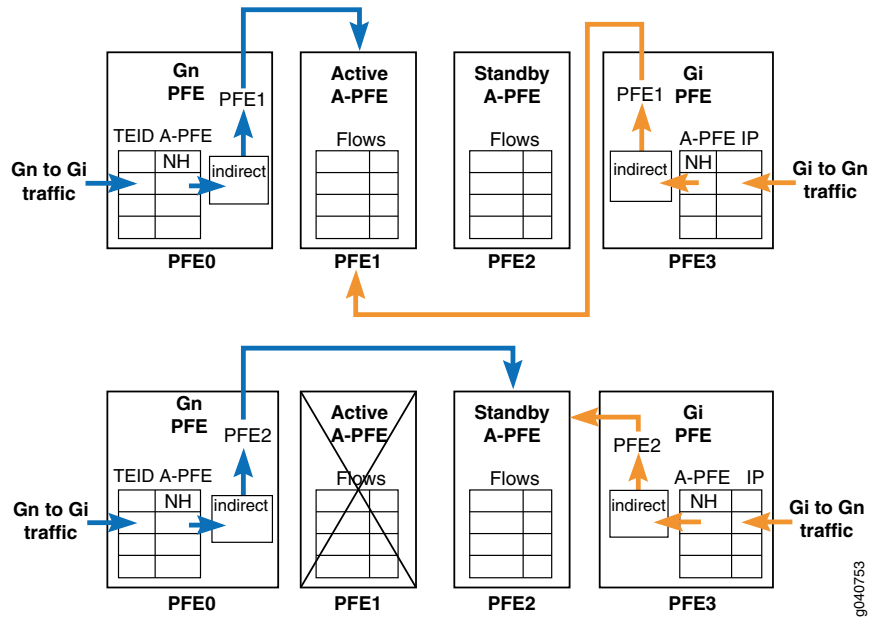
As shown in [Figure 26 on page 80](#), you can configure session DPCs with or without backup. In this case, **MS0** has no backup redundancy, while both PICs (PIC0 and PIC1) on **MS1** are backed up 1:1 by standby **MS2**. When the anchor session DPC **MS1** fails, packets cannot be processed strictly by hardware data path until the transfer of control to the new anchor is complete. This is shown in [Figure 27 on page 81](#). Note that **ams1** now points to **MS2**, the new active anchor.

Figure 27: 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 28 on page 81](#). For clarity, only the active and standby Packet Forwarding Engines are shown.

Figure 28: 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 74](#)
 - [Configuring Session DPC Redundancy on page 76](#)
 - [Configuring Interface Redundancy on page 78](#)
 - [Example: Configuring Broadband Gateway Redundancy on page 82](#)
 - [Configuring Anchor Session DPCs and PFEs on page 71](#)

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 82](#)
- [Overview on page 82](#)
- [Configuration on page 83](#)
- [Verification on page 85](#)

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

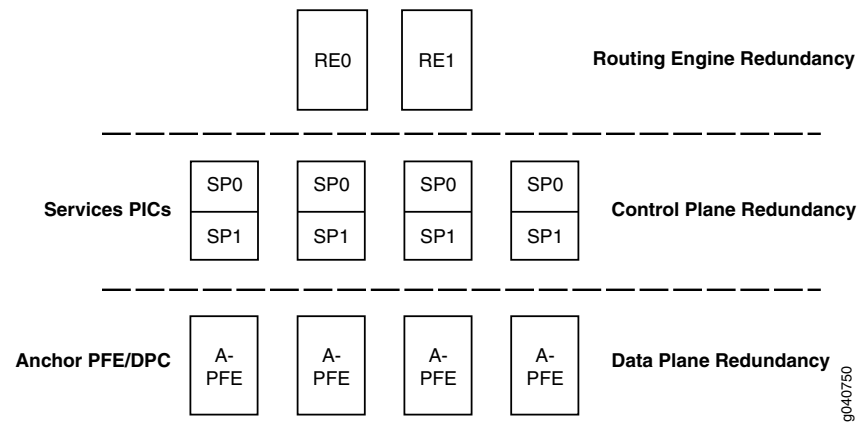
Before you begin:

- Install the chassis hardware.
- Configure the chassis.

Overview

[Figure 29 on page 83](#) 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 29: Redundancy Example for the Broadband Gateway



In this example, the chassis has session DPCs in Packet Forwarding Engines 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. This example backs up Packet Forwarding Engines **pfe-7/0/0** and **pfe-8/0/0** with warm standby **pfe-9/0/0**.

Configuration

Redundancy for the above is configured by:

- [Configuration on page 83](#)

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-interface-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 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;
    member-failure-options {
      drop-member-traffic {
        rejoin-timeout 10000;
      }
    }
    high-availability-options {
      many-to-one {
        preferred-backup mams-5/1/0;
      }
    }
  }
  unit 1 {
    family inet;
  }
  unit 2 {
    family inet;
  }
}

apfe0 {
  anchoring-options {
    primary-list {
```

```

    fpc-7/0/0;
    fpc-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 74](#)
 - [Configuring Session DPC Redundancy on page 76](#)
 - [Configuring Interface Redundancy on page 78](#)
 - [Understanding the Broadband Gateway Anchor Failover Behavior on page 80](#)
 - [Configuring Anchor Session DPCs and PFEs on page 71](#)

CHAPTER 5

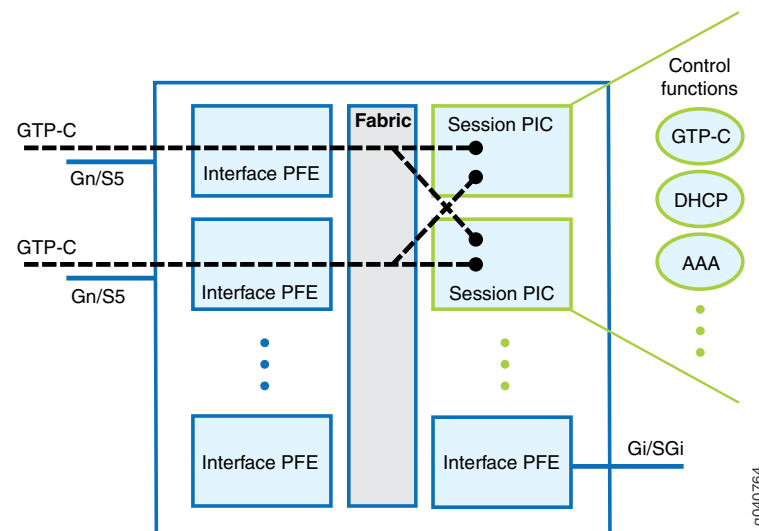
Configuring Mobile Edge Exception Handling

- [Understanding the Broadband Gateway Exception Handling on page 88](#)
- [Understanding GTP-U Error Exception Handling on page 89](#)
- [Understanding Broadband Gateway IP Fragment Handling on page 90](#)
- [Configuring Fragment Reassembly Parameters on page 90](#)
- [Understanding IPv6 Protocol Parameters on page 92](#)
- [Configuring IPv6 Protocol Parameters on page 93](#)
- [Configuring Exception Handling Traceoptions on page 95](#)
- [Configuring S-GW Data Path Traceoptions on page 97](#)
- [Example: Configuring Broadband Gateway Exception Handling Parameters on page 99](#)

Understanding the Broadband Gateway Exception Handling

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. However, certain *exception* packets follow a path through software.

Figure 30: GTP-C Handling



As shown in [Figure 30 on page 88](#), 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 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 Exception Handling on page 89](#)
- [Understanding Broadband Gateway IP Fragment Handling on page 90](#)
- [Configuring Fragment Reassembly Parameters on page 90](#)
- [Understanding IPv6 Protocol Parameters on page 92](#)
- [Configuring IPv6 Protocol Parameters on page 93](#)
- [Configuring Exception Handling Traceoptions on page 95](#)
- [Configuring S-GW Data Path Traceoptions on page 97](#)
- [Example: Configuring Broadband Gateway Exception Handling Parameters on page 99](#)

Understanding GTP-U Error Exception Handling

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 Exception Handling on page 88](#)
- [Understanding Broadband Gateway IP Fragment Handling on page 90](#)
- [Configuring Fragment Reassembly Parameters on page 90](#)
- [Understanding IPv6 Protocol Parameters on page 92](#)
- [Configuring IPv6 Protocol Parameters on page 93](#)
- [Configuring Exception Handling Traceoptions on page 95](#)
- [Configuring S-GW Data Path Traceoptions on page 97](#)
- [Example: Configuring Broadband Gateway Exception Handling Parameters on page 99](#)

Understanding Broadband Gateway 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. You can control many of the parameters associated with the 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.

Related Documentation

- [Understanding the Broadband Gateway Exception Handling on page 88](#)
- [Understanding GTP-U Error Exception Handling on page 89](#)
- [Configuring Fragment Reassembly Parameters on page 90](#)
- [Understanding IPv6 Protocol Parameters on page 92](#)
- [Configuring IPv6 Protocol Parameters on page 93](#)
- [Configuring Exception Handling Traceoptions on page 95](#)
- [Configuring S-GW Data Path Traceoptions on page 97](#)
- [Example: Configuring Broadband Gateway Exception Handling Parameters on page 99](#)

Configuring Fragment Reassembly Parameters

On the MobileNext Broadband Gateway, anchor session Dense Port Concentrators (DPCs) reassemble arriving user plane packet fragment 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 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 reassembly-profile-one ]
user@host# set timeout 2
```



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

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

```
[edit services ip-reassembly reassembly-profile-one ]
user@host# set max-reassembly-pending-packets 100
```



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

Related Documentation

- [Understanding the Broadband Gateway Exception Handling on page 88](#)
- [Understanding GTP-U Error Exception Handling on page 89](#)
- [Understanding Broadband Gateway IP Fragment Handling on page 90](#)
- [Understanding IPv6 Protocol Parameters on page 92](#)
- [Configuring IPv6 Protocol Parameters on page 93](#)
- [Configuring Exception Handling Traceoptions on page 95](#)
- [Configuring S-GW Data Path Traceoptions on page 97](#)
- [Example: Configuring Broadband Gateway Exception Handling Parameters on page 99](#)

Understanding IPv6 Protocol Parameters

The MobileNext Broadband Gateway supports 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

- [Understanding the Broadband Gateway Exception Handling on page 88](#)
- [Understanding GTP-U Error Exception Handling on page 89](#)
- [Understanding Broadband Gateway IP Fragment Handling on page 90](#)
- [Configuring Fragment Reassembly Parameters on page 90](#)
- [Configuring IPv6 Protocol Parameters on page 93](#)
- [Configuring Exception Handling Traceoptions on page 95](#)
- [Configuring S-GW Data Path Traceoptions on page 97](#)
- [Example: Configuring Broadband Gateway Exception Handling Parameters on page 99](#)

Configuring IPv6 Protocol 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 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 10
```



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. There is no default.

.....

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 the Broadband Gateway Exception Handling on page 88](#)
- [Understanding GTP-U Error Exception Handling on page 89](#)
- [Understanding Broadband Gateway IP Fragment Handling on page 90](#)
- [Configuring Fragment Reassembly Parameters on page 90](#)
- [Understanding IPv6 Protocol Parameters on page 92](#)
- [Configuring Exception Handling Traceoptions on page 95](#)
- [Configuring S-GW Data Path Traceoptions on page 97](#)
- [Example: Configuring Broadband Gateway Exception Handling Parameters on page 99](#)

Configuring Exception Handling Traceoptions

Datapath tracing operations record detailed messages about the operation of exception-handling services such as packet reassembly or IPv6 router advertisements on the MobileNext Broadband Gateway. You can trace various types of exception 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 12 on page 95 describes the flags relating to the exceptions that you can include at the `[edit unified-edge gateways ggsn-pgw gateway-name software-datapath traceoptions flag]` hierarchy level.

Table 12: Trace Flags

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

Table 13 on page 95 describes the levels you can include.

Table 13: Trace Levels

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

Table 13: Trace Levels (*continued*)

verbose	Match verbose messages.
warning	Match warning messages.

To configure tracing options for exception operations:

1. Specify that you want to configure tracing options for exception 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, exception-log) reaches its maximum size, it is renamed exception-log.0, then exception-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/exception-log
```

Related Documentation

- [Understanding the Broadband Gateway Exception Handling on page 88](#)
- [Understanding GTP-U Error Exception Handling on page 89](#)
- [Understanding Broadband Gateway IP Fragment Handling on page 90](#)
- [Configuring Fragment Reassembly Parameters on page 90](#)
- [Understanding IPv6 Protocol Parameters on page 92](#)

- [Configuring IPv6 Protocol Parameters on page 93](#)
- [Configuring S-GW Data Path Traceoptions on page 97](#)
- [Example: Configuring Broadband Gateway Exception Handling Parameters on page 99](#)

Configuring S-GW 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 14 on page 97](#) describes the flags relating to the exceptions that you can include at the `[edit unified-edge gateways sgw gateway-name software-datapath traceoptions flag]` hierarchy level.

Table 14: 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 15 on page 97](#) describes the levels you can include.

Table 15: S-GW Datapath Trace Levels

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

Table 15: S-GW Datapath Trace Levels (*continued*)

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

To configure tracing options for datapath operations:

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

```
[edit unified-edge gateways sgw MBG2 software-datapath]
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 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
```



NOTE: When a trace file (for example, `datapath-log`) reaches its maximum size, it is renamed `datapath-log.0`, then `datapath-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 sgw MBG2 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 sgw MBG2 software-datapath traceoptions]
user@host# set level error
```

6. View the trace file.

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


Related Documentation

- [Understanding the Broadband Gateway Exception Handling on page 88](#)
- [Understanding GTP-U Error Exception Handling on page 89](#)
- [Understanding Broadband Gateway IP Fragment Handling on page 90](#)
- [Configuring Fragment Reassembly Parameters on page 90](#)
- [Understanding IPv6 Protocol Parameters on page 92](#)
- [Configuring IPv6 Protocol Parameters on page 93](#)
- [Configuring Exception Handling Traceoptions on page 95](#)
- [Configuring S-GW Traceoptions on page 33](#)
- [Configuring S-GW GTP Traceoptions on page 262](#)
- [Configuring S-GW Charging Traceoptions on page 284](#)
- [Configuring S-GW Local Persistent Storage Traceoptions on page 287](#)

Example: Configuring Broadband Gateway Exception Handling Parameters

This example shows how to configure exception handling parameters on the MobileNext Broadband Gateway. Both IP reassembly and IPv6 advertisement parameters are configured.

- [Requirements on page 99](#)
- [Overview on page 100](#)
- [Configuration on page 100](#)
- [Verification on page 101](#)

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

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 IP fragment reassembly and IPv6 router advertisements. The 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.

Configuration

The parameters for IP fragment reassembly and IPv6 router advertisements are configured by:

- [\[xref target has no title\]](#)

CLI Quick Configuration

```
[edit services ip-reassembly reassembly-profile-one]
set timeout 2 # The default (seconds)
set max-reassembly-pending-packets 100 # The default
```

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

```
[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 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;
}
```

```
show unified-edge gateways ggsn-pgw MBG1 ip-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 IP Reassembly Configuration

Purpose	Verify that IP reassembly exception handling is operating.
Action	From operational mode, enter the show unified-edge gateways ggsn-pgw ip-reassembly statistics command.
Meaning	Non-zero values indicate that reassembly is functioning.



NOTE: You must inspect IPv6 router advertisement packets directly to verify configured header field parameters.

Verifying the Exception Handling Configuration

Purpose	Verify that exception handling is operating.
Action	From operational mode, enter the show unified-edge gateways ggsn-pgw exception-handling statistics command.



NOTE: You can clear these statistics with the **clear unified-edge gateways ggsn-pgw exception-handling statistics** command.

Meaning	Non-zero values indicate that exception handling is functioning.
----------------	--

Related Documentation	<ul style="list-style-type: none"> • Understanding the Broadband Gateway Exception Handling on page 88 • Understanding GTP-U Error Exception Handling on page 89
------------------------------	--

- [Understanding Broadband Gateway IP Fragment Handling on page 90](#)
- [Configuring Fragment Reassembly Parameters on page 90](#)
- [Understanding IPv6 Protocol Parameters on page 92](#)
- [Configuring IPv6 Protocol Parameters on page 93](#)
- [Configuring Exception Handling Traceoptions on page 95](#)
- [Configuring S-GW Data Path Traceoptions on page 97](#)

PART 3

APN Configuration

- [Configuring APNs on page 105](#)

CHAPTER 6

Configuring APNs

- [Configuring APNs on the MobileNext Broadband Gateway Overview on page 105](#)
- [User-Session Routing Overview on page 107](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 109](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 113](#)
- [Configuring Anonymous Users on a Broadband Gateway APN on page 114](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 115](#)
- [Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 119](#)
- [Configuring Mobile Interfaces for APNs on page 120](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 122](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 123](#)
- [Example: Configuring Broadband Gateway APNs on page 126](#)
- [Networks Behind the Mobile Device Overview on page 130](#)
- [Configuring the Networks Behind the Mobile Equipment Feature on page 131](#)
- [Example: Configuring the Networks Behind the Mobile Device Feature on page 133](#)
- [HTTP Header Enrichment Overview on page 134](#)
- [Configuring HTTP Header Enrichment on page 135](#)
- [Example: Configuring HTTP Header Enrichment on page 138](#)

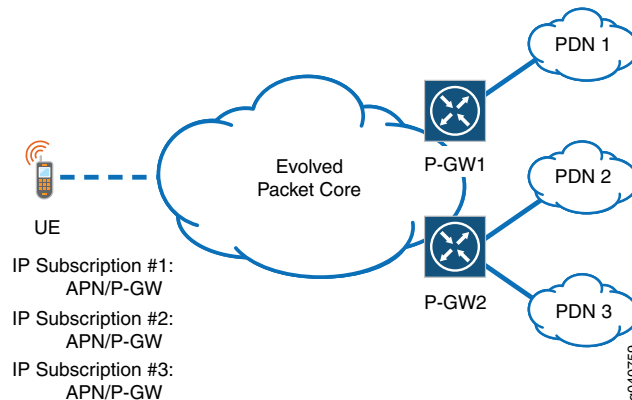
Configuring APNs on the MobileNext Broadband Gateway Overview

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 31 on page 106](#) shows the relationship between APNs and broadband gateways in a 4G network.

Figure 31: 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
- Anonymous users
- 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.

Anonymous Users

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 General APN Parameters on the Broadband Gateway on page 109](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 113](#)
- [Configuring Anonymous Users on a Broadband Gateway APN on page 114](#)
- [Configuring Anonymous Users on a Broadband Gateway APN on page 114](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 115](#)
- [Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 119](#)
- [Configuring Mobile Interfaces for APNs on page 120](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 122](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 123](#)
- [Example: Configuring Broadband Gateway APNs on page 126](#)

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 123](#)
- [Configuring APNs on the MobileNext Broadband Gateway Overview on page 105](#)

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 109](#)
- [Configuring Servers for an APN on page 110](#)
- [Configuring APN Timers on page 111](#)
- [Configuring Miscellaneous APN Parameters on page 111](#)

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**—The mobile station or network provides the APN name, and the subscription to the APN is verified.
- **from-sgsn**—The mobile station provides the APN name, and the subscription to the APN is not verified.
- **no-subscribed**—The network provides the APN name, and the subscription to the APN is not verified. The gateway will not accept a session for a subscriber with this APN name set in the mobile device, even if verified and subscribed.

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
```

8. Configure the default APN, which is used when a create session message does not include the APN name.

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



NOTE: If no default APN is configured, and the create session message does not include an APN name, the session is rejected.

Related Documentation

- [Configuring APNs on the MobileNext Broadband Gateway Overview on page 105](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 113](#)
- [Configuring Anonymous Users on a Broadband Gateway APN on page 114](#)
- [Configuring Anonymous Users on a Broadband Gateway APN on page 114](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 115](#)
- [Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 119](#)
- [Configuring Mobile Interfaces for APNs on page 120](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 122](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 123](#)
- [Example: Configuring Broadband Gateway APNs on page 126](#)

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 16 on page 114](#) 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 16: 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
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 APNs on the MobileNext Broadband Gateway Overview on page 105](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 109](#)
- [Configuring Anonymous Users on a Broadband Gateway APN on page 114](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 115](#)
- [Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 119](#)
- [Configuring Mobile Interfaces for APNs on page 120](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 122](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 123](#)
- [Example: Configuring Broadband Gateway APNs on page 126](#)

Configuring Anonymous Users on a Broadband Gateway APN

Before you begin configuring anonymous user parameters 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

To verify anonymous users on the broadband gateway, you configure a default username and password for authentication. Without this username and password, the broadband gateway does not accept anonymous users. You also specify a method to use for

verification to prevent fraud using the device's International Mobile Station Identity (IMSI), Mobile Subscriber Integrated Services Digital Network (MSISDN) number, or APN name.

To configure anonymous user parameters on a broadband gateway APN:

1. Configure the username and verification method for anonymous users on **apn-1**.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1 anonymous-user]
user@host# set user-name use-apnname user-name
```



NOTE: Alternatively, you can configure `set use-msdn`, `set use-apnname`, or `set use-imsi` as an anonymous username for authentication. There is no default name.

2. Configure the password for anonymous users on **apn-1**:

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1 anonymous-user]
user@host# set password 2*20!s550
```



NOTE: The password can be up to 32 characters long.

Related Documentation

- [Configuring APNs on the MobileNext Broadband Gateway Overview on page 105](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 109](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 113](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 115](#)
- [Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 119](#)
- [Configuring Mobile Interfaces for APNs on page 120](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 122](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 123](#)
- [Example: Configuring Broadband Gateway APNs on page 126](#)

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

To assign IP addresses to devices accessing the broadband gateway APN, you configure a DHCP IPv4 and IPv6 proxy client based on DHCP profiles. The address pools can be included in or excluded from the APN. You can also configure parameters for static address use and authentication, authorization, and accounting (AAA).

To configure address assignment on a broadband gateway APN:

1. Configure address assignment to use AAA on **apn-1**.

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

2. Configure address assignment to allow user equipment to provide a static address that is not verified by AAA on **apn-1**.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
address-assignment]
user@host# set allow-static-ip-address no-aaa-verify
```

3. Configure AAA to override the address received by the DHCP proxy client for this APN.

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

4. Optionally, configure the logical system 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 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.

5. Optionally, configure the address pool name 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 pool-name pool-name
```



NOTE: This is the name of the address pool sent to the DHCP server.

6. Configure the profile name 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 profile-name profile-name
```



NOTE: The DHCPv6 profile parameters must be defined.

7. Optionally, 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
```



NOTE: This is the routing instance where the DHCPv4 proxy client profile is defined. If this is not specified, the default routing instance is used.

8. Optionally, configure the logical system 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 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.

9. Optionally, configure the address pool name 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 pool-name pool-name
```



NOTE: This is the name of the address pool sent to the DHCP server.

10. Configure the profile name 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 profile-name profile-name
```



NOTE: The DHCPv6 profile parameters must be defined.

11. Optionally, 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 dhcpv6-proxy-client-profile routing-instance routing-instance-name
```



NOTE: This is the routing instance where the DHCPv4 proxy client profile is defined. If this is not specified, the default routing instance is used.

12. Configure the IPv4 address pool or group for this APN.

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



NOTE: The address pool or group referenced must be defined.

13. Configure one or more IPv4 address pools to exclude for this APN.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
 address-assignment]
user@host# set inet-pool exclude-pools pool-name(s)
```



NOTE: The address pool or group referenced must be defined.

14. Configure the IPv6 address pool or group for this APN.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
 address-assignment]
user@host# set inet6-pool pool pool-name
user@host# set inet6-pool group group-name
```



NOTE: The address pool or group referenced must be defined.

15. Configure one or more IPv6 address pools to exclude for this APN.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-1
 address-assignment]
user@host# set inet6-pool exclude-v6pools v6pool-name(s)
```



NOTE: The address pool or group referenced must be defined.

16. Optionally, configure AAA to override local address assignment for this APN.

```
user@host# set local aaa-override
```

Related Documentation

- [Configuring APNs on the MobileNext Broadband Gateway Overview on page 105](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 109](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 113](#)
- [Configuring Anonymous Users on a Broadband Gateway APN on page 114](#)

- [Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 119](#)
- [Configuring Mobile Interfaces for APNs on page 120](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 122](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 123](#)
- [Example: Configuring Broadband Gateway APNs on page 126](#)

Configuring Charging and Local Policy 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 details and quality-of-service (QoS) local policy profiles 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.

Related Documentation

- [Configuring APNs on the MobileNext Broadband Gateway Overview on page 105](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 109](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 113](#)
- [Configuring Anonymous Users on a Broadband Gateway APN on page 114](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 115](#)
- [Configuring Mobile Interfaces for APNs on page 120](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 122](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 123](#)
- [Example: Configuring Broadband Gateway APNs on page 126](#)

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:

- Configure the logical interface.

```
[edit interfaces]
user@host# set mif unit 0 family inet
```

- 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.

- 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.

- 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 APNs on the MobileNext Broadband Gateway Overview on page 105](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 109](#)

- [Configuring the Restriction Value on a Broadband Gateway APN on page 113](#)
- [Configuring Anonymous Users on a Broadband Gateway APN on page 114](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 115](#)
- [Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 119](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 122](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 123](#)
- [Example: Configuring Broadband Gateway APNs on page 126](#)

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 APNs on the MobileNext Broadband Gateway Overview on page 105](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 109](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 113](#)
- [Configuring Anonymous Users on a Broadband Gateway APN on page 114](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 115](#)
- [Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 119](#)
- [Configuring Mobile Interfaces for APNs on page 120](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 123](#)
- [Example: Configuring Broadband Gateway APNs on page 126](#)

Configuring APN Service Selection on a Broadband Gateway

The MobileNext Broadband Gateway can select an access point name (APN) in various ways. You configure an APN service selection method as an “if-then” construction similar to other Junos OS policies using **from** and **then** statements.

Before you begin configuring APN 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 an APN selection method, you can choose one or more of the following **from** conditions:

- **charging-characteristics value**—Match the charging characteristics value from 1 through 65,535 to select the APN.
- **imei imei-prefix**—Use the International Mobile Equipment Identity (IMEI) prefix configured to select the APN.
- **imsi imsi-prefix**—Use the International Mobile Subscriber Identity (IMSI) prefix configured to select the APN.
- **maximum-bearers value**—Match the number of bearers in the gateway from 1 through 10,000,000 (10 million) to select the APN.
- **msisdn msisdn-number-prefix**—Use the Mobile Station Integrated Services Digital Network (MSISDN) prefix configured to select the APN.
- **pdn-type [ipv4 | ipv6 | ipv4v6]**—Use the IP version configured to select the APN.
- **peer ip-address**—Use the IP address of the peer creating the session to select the APN.
- **peer-routing-instance routing-instance-name**—Use the routing instance of the peer creating the session to select the APN.



NOTE: Multiple terms can be configured in a 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.

The remaining statements are explained separately.

To configure an APN selection method, you can choose one of the following **then** conditions:

- **apn-name** *apn-name*—Select this real APN name.
- **redirect-peer** *ip-address*—Select this redirected peer address to access the APN.

To configure APN service selection **from** statements on a broadband gateway:

1. Configure the **charging-characteristics** **from** method in a term called *select-apn* in a selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles profile
  apn-1-selection term select-apn]
user@host# set from charging-characteristics 12345
```

2. Configure the **imei** **from** method in a term called *select-apn* in a selection profile called *apn-1-selection*.



NOTE: Terms can be up to 63 characters long.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles profile
  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.

3. Configure the **imsi** **from** method in a term called *select-apn* in a selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles profile
  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.

4. Configure the **maximum-bearers from** method in a term called *select-apn* in a selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles profile
  apn-1-selection term select-apn]
user@host# set from maximum-bearers 123456
```

5. Configure the **msisdn from** method in a term called *select-apn* in a selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles profile
  apn-1-selection term select-apn]
user@host# set from msisdn msisdn-number-prefix
```



NOTE: The MS-ISDN prefix matches the specified digits. For example, from msisdn 1212555 matches the first seven digits as given, then any other digits.

6. Configure the **pdn-type from** method in a term called *select-apn* in a selection method called *apn-1-selection*.

```
[edit unified-edge apn-service-selection apn-1-selection term select-apn]
user@host# set from pdn-type [ ipv4 | ipv6 | ipv4v6 ]
```

7. Configure the **peer from** method in a term called *select-apn* in a selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles profile
  apn-1-selection term select-apn]
user@host# set from peer 192.168.1.20
```

8. Configure the **peer-routing-instance from** method in a term called *select-apn* in a selection profile called *apn-1-selection*.

```
[edit unified-edge gateways ggsn-pgw MBG1 service-selection-profiles profile
  apn-1-selection term select-apn]
user@host# set from peer-routing-instance mobility-instance
```

To configure APN service selection **then** statements on a broadband gateway:

1. Configure the **apn-name then** method in a term called *select-apn* in a selection method called *apn-1-selection*.

```
[edit unified-edge apn-service-selection apn-1-selection term select-apn]
user@host# set then apn-name MBG1-apn
```

2. Alternatively, configure the **redirect-peer ip-address then** method in a term called *select-apn* in a selection method called *apn-1-selection*.

```
[edit unified-edge apn-service-selection apn-1-selection term select-apn]
user@host# set then redirect-peer 192.168.20.1
```

Related Documentation

- [Configuring APNs on the MobileNext Broadband Gateway Overview on page 105](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 109](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 113](#)

- [Configuring Anonymous Users on a Broadband Gateway APN on page 114](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 115](#)
- [Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 119](#)
- [Configuring Mobile Interfaces for APNs on page 120](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 122](#)
- [Example: Configuring Broadband Gateway APNs on page 126](#)

Example: Configuring Broadband Gateway APNs

This example shows how to configure an access point name (APN) on the MobileNext Broadband Gateway. An APN selection method is configured, along with a mobile interface (**mif-**). The APN interfaces are placed into a virtual routing and forwarding (VRF) routing instance.

- [Requirements on page 126](#)
- [Overview on page 126](#)
- [Configuration on page 127](#)
- [Verification on page 129](#)

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 DPCs or Modular Port Concentrators [MPCs]).
- The Junos OS Mobility package software

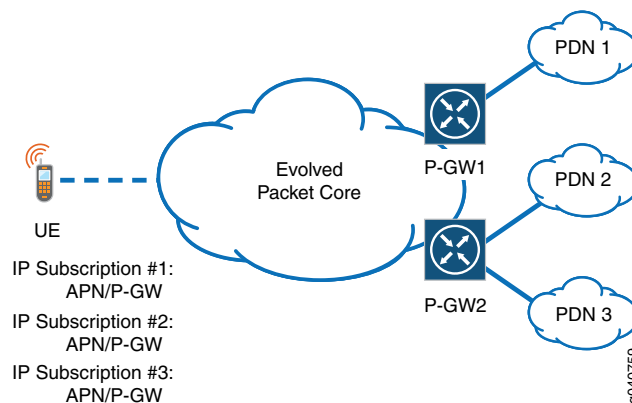
Before you begin:

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

Overview

[Figure 32 on page 127](#) 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 32: 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, but a selection method is still required. The mobile interface is configured (**mif.0**), 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-1/0/1.0** and is a real APN. The APN includes Domain Name System (DNS) and call state control function (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 AAA mobility hierarchy level). All other general APN parameters either use the default values or are not configured.

This APN configuration places no restrictions of traffic sent from one APN to another (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 group is **group-1-apn-1** and the pool is called **pool-1**. 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

The APN referenced above is configured by:

CLI Quick Configuration

```
[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-server 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 group group-1-apn-1
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.1
user@host# set User1-VRF interface ge-0/0/0.5

[edit unified-edge apn-service-selection apn-1-selection term select-apn]
user@host# set from
[edit unified-edge apn-service-selection apn-1-selection term select-apn]
user@host# set then apn-service apn-1
```

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 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-cssf server 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 {
    group group-1-apn-1;
    pool pool-1;
  }
}
```

```

charging {
  default-charging-profile default-charging-profile-apn-1;
}

show interfaces
mif {
  unit 0 {
    family inet;
  }
}

show routing-instances User1-VRF interfaces
mif-0;
ge-0/0/0.5;

show unified-edge apn-service-selection apn-1-selection
term select-apn {
  from;
  then {
    apn-service apn-1;
  }
}

```

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

Verification

Verifying the APN Configuration

Purpose	Verify that the APN is configured or not.
Action	From operational mode, enter the show unified-edge ggsn-pgw apn statistics apn-name apn-1 command.
Meaning	The APN configured (apn-1 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.
Related Documentation	<ul style="list-style-type: none"> • Configuring APNs on the MobileNext Broadband Gateway Overview on page 105 • Configuring General APN Parameters on the Broadband Gateway on page 109 • Configuring the Restriction Value on a Broadband Gateway APN on page 113 • Configuring Anonymous Users on a Broadband Gateway APN on page 114 • Configuring Address Assignment on a Broadband Gateway APN on page 115 • Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 119 • Configuring Mobile Interfaces for APNs on page 120 • Configuring Mobile Interface to APN Associations in VRFs on page 122

- [Configuring APN Service Selection on a Broadband Gateway on page 123](#)

Networks Behind the Mobile Device Overview

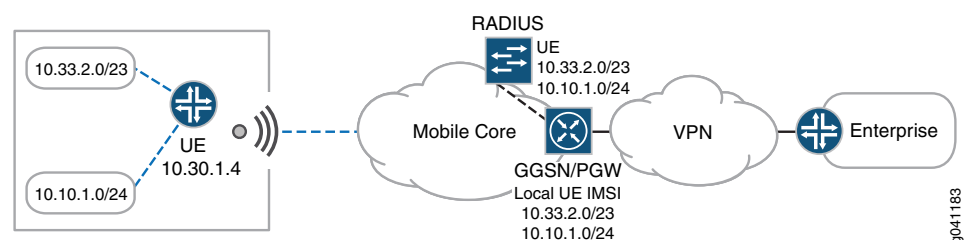
The fundamental function of a MobileNext Broadband Gateway configured as a Gateway GPRS Support Node (GGSN) or Packet Data Network Gateway (P-GW) is to provide IP connectivity and services to the mobile subscriber. In small office, home office (SOHO) environments, the mobile user equipment can act as 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 33 on page 130](#) 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 (10.30.1.4). These addresses can be obtained locally or through a RADIUS server (both are shown in the figure).

Figure 33: 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 131](#)
- [Example: Configuring the Networks Behind the Mobile Device Feature on page 133](#)

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 RADIUS, this is the only step required. You must also configure the RADIUS server.

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. (Option) 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. (Option) 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

- [Networks Behind the Mobile Device Overview on page 130](#)
- [Example: Configuring the Networks Behind the Mobile Device Feature on page 133](#)

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 133](#)
- [Overview on page 133](#)
- [Configuration on page 133](#)
- [Verification on page 134](#)

Requirements

This example uses the following hardware and software components:

- An MX Series chassis (except the MX180) 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

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 **111222330012347**.

Configuration

The networks behind the mobile equipment feature referenced above is configured by:

CLI Quick Configuration	<pre>[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns nbm-apn] user@host# set mobile-interface <i>mif.0</i> user@host# set allow-network-behind-mobile user@host# set address-assignment <i>local</i></pre>
----------------------------	--

```
user@host# set network-behind-mobile imsi 111222330012347 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** from configuration mode.

Verification

Verifying the Networks Behind the Mobile Equipment Configuration

Purpose	Verify that a mobile subscriber is associated with the configured network-behind-mobile prefixes.
Action	From operational mode, enter the show unified-edge ggsn-pgw gateway MBG1 subscribers extensive command.
Meaning	The output associated with the IMSI (111222330012347 in this case) displays a list of IPv4 addresses as IPv4 NBM address (although the prefixes are listed for the APN nbm-apn).
Related Documentation	<ul style="list-style-type: none">• Networks Behind the Mobile Device Overview on page 130• Configuring the Networks Behind the Mobile Equipment Feature on page 131

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 135](#)
 - [Example: Configuring HTTP Header Enrichment on page 138](#)

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 134](#)
 - [Example: Configuring HTTP Header Enrichment on page 138](#)

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 138](#)
- [Overview on page 138](#)
- [Configuration on page 139](#)
- [Verification on page 144](#)

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 service-set-1;  
        }  
        output {  
          service-set service-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 134](#)
- [Configuring HTTP Header Enrichment on page 135](#)

PART 4

Authorization and Addressing Configuration

- [Configuring AAA on page 147](#)
- [Configuring DHCP on page 207](#)

CHAPTER 7

Configuring AAA

- Overview of AAA on the Broadband Gateway on page 148
- Scalability and Redundancy on page 150
- Network Elements on page 151
- Network Element Groups on page 152
- AAA Profiles on page 153
- Supported Attributes in Access-Request Messages on page 155
- Supported Attributes in Access-Accept Messages on page 159
- Supported Attributes in Accounting Start Messages on page 162
- Supported Attributes in Accounting Interim Update Messages on page 166
- Supported Attributes in Accounting Stop Messages on page 171
- Supported Attributes in Accounting On Messages on page 175
- Supported Attributes in Disconnect Request Messages on page 176
- Supported Attributes in Change of Authorization (CoA) Messages on page 177
- Configuring AAA on the Broadband Gateway on page 179
- Configuring Interaction Between the Broadband Gateway and RADIUS Servers on page 179
- Configuring RADIUS-Initiated Dynamic Request Support on page 181
- Configuring Dead Server Detection on page 181
- Configuring Network Elements on page 182
- Configuring Network Element Groups on page 183
- Configuring an AAA Profile on page 184
- Configuring Authentication Settings in an AAA Profile on page 184
- Configuring Accounting Settings in an AAA Profile on page 185
- Configuring RADIUS Attribute Usage for an AAA Profile on page 186
- Specifying RADIUS Options in an AAA Profile on page 190
- Applying an AAA Profile to an APN on page 190
- Enabling Address Assignment by the RADIUS Server on page 191

- [Configuring AAA-Assigned Addresses to Override Locally or DHCP-Assigned Addresses on page 191](#)
- [Configuring the Broadband Gateway to Wait for an Accounting Response on page 192](#)
- [Example: Configuring AAA on the Broadband Gateway on page 192](#)

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, then the option specified for the **user-name** parameter in the **anonymous-user** statement of the access point name (APN) configuration is used instead. This can be an actual username, 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, the password specified for the **password** setting in the **anonymous-user** statement is used instead.

- For the Challenge Handshake Authentication Protocol (CHAP), 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 177](#) 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 176](#) 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 155](#) and [“Supported Attributes in Access-Accept Messages” on page 159](#) describe how the broadband gateway processes these attributes and VSAs.

Related Documentation

- [Configuring APNs on the MobileNext Broadband Gateway Overview on page 105](#)
- [Configuring AAA on the Broadband Gateway on page 179](#)
- [Configuring Anonymous Users on a Broadband Gateway APN on page 114](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 115](#)
- [Example: Configuring AAA on the Broadband Gateway on page 192](#)

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 62](#)
- [Broadband Gateway Redundancy Overview on page 74](#)
- [Network Elements on page 151](#)
- [Network Element Groups on page 152](#)

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 153](#)
- [Configuring Network Elements on page 182](#)
- [Network Element Groups on page 152](#)

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 153](#)
- [Configuring Network Elements on page 182](#)
- [Configuring Network Element Groups on page 183](#)

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 184](#)
- [Configuring Network Elements on page 182](#)
- [Configuring Network Element Groups on page 183](#)

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 for authenticating a user.

- [RADIUS IETF Attributes Supported in Access-Request Messages on page 155](#)
- [3GPP VSAs Supported in Access-Request Messages on page 157](#)

RADIUS IETF Attributes Supported in Access-Request Messages

Table 17 on page 155 lists the RADIUS attributes supported by the broadband gateway in Access-Request messages.

Table 17: 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 the PPP PDP type is used, it is provided to the broadband gateway by the user during the PPP authentication phase.</p> <p>If no username is available, then the option specified for the user-name parameter in the anonymous-user statement of the APN configuration is used instead.</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 the PPP PDP type is used, it is provided to the broadband gateway by the user during the PPP authentication phase.</p> <p>If no user password is available, then the password specified for the password parameter in the anonymous-user statement of the APN configuration is used instead.</p>	String

Table 17: RADIUS IETF Attributes Supported in Access-Request Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
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) or PPP authentication phase (if the PPP PDP type is used).	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
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	<p>The CHAP Challenge is provided to the broadband gateway by the user in the PCO received during the IP-CAN session establishment procedure.</p> <p>If the PPP PDP type is used, it is provided to the broadband gateway by the user during the PPP authentication phase.</p>	String

Table 17: RADIUS IETF Attributes Supported in Access-Request Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
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 18 on page 157 lists the 3GPP vendor-specific attributes (VSAs) supported by the broadband gateway in Access-Request messages.

Table 18: 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
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
26/10415/4	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-PS-Negotiated-QoS-Profile	QoS profile applied by the broadband gateway for the PDP context/EPS bearer.	UTF-8 encoded string

Table 18: 3GPP VSAs Supported in Access-Request 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/EPS bearer, received in the Create PDP Context/Session Request message.	String

Table 18: 3GPP VSAs Supported in Access-Request Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
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
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

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 160](#)
- [3GPP VSAs Supported in Access-Accept Messages on page 161](#)
- [Juniper Networks VSAs Supported in Access-Accept Messages on page 162](#)

RADIUS IETF Attributes Supported in Access-Accept Messages

[Table 19 on page 160](#) lists the RADIUS attributes supported by the broadband gateway in Access-Accept messages.

Table 19: 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
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

Table 19: RADIUS IETF Attributes Supported in Access-Accept Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
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
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 21 on page 162 lists the 3GPP vendor-specific attributes (VSAs) supported by the broadband gateway in Access-Accept messages.

Table 20: 3GPP VSAs Supported in Access-Accept Messages

Attribute Number	Attribute Name	Description	Content
26/10415/5	3GPP-PS-Negotiated-QoS-Pro	QoS profile applied by the broadband gateway for the PDP context/EPS bearer.	UTF-8 encoded string

Table 20: 3GPP VSAs Supported in Access-Accept Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
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 21 on page 162](#) lists the Juniper Networks VSAs supported by the broadband gateway in Access-Accept messages.

Table 21: Juniper VSAs Supported in Access-Accept Messages

Attribute Number	Attribute Name	Description	Content
26-JNPR-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-JNPR-162	Redirect-Gw-Addr	Address of the gateway to which the user session should be redirected.	IPv4 address
26-JNPR-163	APN-Name	Name of the APN.	String

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 QoS parameters associated with the session.

- [RADIUS IETF Attributes Supported in Accounting Start Messages on page 162](#)
- [3GPP VSAs Supported in Accounting Start Messages on page 164](#)

RADIUS IETF Attributes Supported in Accounting Start Messages

[Table 22 on page 163](#) lists the RADIUS attributes supported by the broadband gateway in Accounting Start messages.

Table 22: 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 the PPP PDP type is used, it is provided to the broadband gateway by the user during the PPP authentication phase.</p> <p>If no username is available, then the option specified for the user-name parameter in the anonymous-user statement of the APN configuration is used instead.</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 22: RADIUS IETF Attributes Supported in Accounting Start Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
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 23 on page 164 lists the 3GPP vendor-specific attributes (VSAs) supported by the broadband gateway in Accounting Start messages.

Table 23: 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-Profiles	QoS profile applied by the broadband gateway for the PDP context/EPS bearer	UTF-8 encoded string

Table 23: 3GPP VSAs Supported in Accounting Start 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/EPS bearer, received in the Create PDP Context/Session Request message.	String

Table 23: 3GPP VSAs Supported in Accounting Start Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
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

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 166](#)
- [3GPP VSAs Supported in Interim-Update Messages on page 168](#)

RADIUS IETF Attributes Supported in Interim-Update Messages

Table 24 on page 167 lists the RADIUS attributes supported by the broadband gateway in Interim-Update messages.

Table 24: 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 the PPP PDP type is used, it is provided to the broadband gateway by the user during the PPP authentication phase.</p> <p>If no username is available, then the option specified for the user-name parameter in the anonymous-user statement of the APN configuration is used instead.</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 24: RADIUS IETF Attributes Supported in Accounting Interim-Update 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 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
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 25 on page 169 lists the 3GPP vendor-specific attributes (VSAs) supported by the broadband gateway in Interim-Update messages.

Table 25: 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/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/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

Table 25: 3GPP VSAs Supported in Accounting Interim-Update Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
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	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
26/10415/21	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

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 171](#)
- [3GPP VSAs Supported in Accounting Stop Messages on page 173](#)

RADIUS IETF Attributes Supported in Accounting Stop Messages

Table 26 on page 171 lists the RADIUS attributes supported by the broadband gateway in Accounting Stop messages.

Table 26: 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 the PPP PDP type is used, it is provided to the broadband gateway by the user during the PPP authentication phase.</p> <p>If no username is available, then the option specified for the user-name parameter in the anonymous-user statement of the APN configuration is used instead.</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

Table 26: RADIUS IETF Attributes Supported in Accounting Stop Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
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 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 26: RADIUS IETF Attributes Supported in Accounting Stop Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
49	Acct-Terminate-Cause	Reason the session was terminated. The session can be terminated for the following reasons: <ul style="list-style-type: none"> • User Request (1)—User initiated the disconnect (log out). • NAS Error (9)—Negotiation failures, connection failures, or address lease expiration. • 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. 	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
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 27 on page 173 lists the 3GPP vendor-specific attributes (VSAs) supported by the broadband gateway in Accounting Stop messages.

Table 27: 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

Table 27: 3GPP VSAs Supported in Accounting Stop Messages (*continued*)

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
26/10415/6	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

Table 27: 3GPP VSAs Supported in Accounting Stop Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
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
26/10415/21	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

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 175](#)

RADIUS IETF Attributes Supported in Accounting On Messages

[Table 28 on page 176](#) lists the RADIUS attributes supported by the broadband gateway in Accounting On messages.

Table 28: 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

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 176](#)
- [3GPP VSAs Supported in Disconnect Request Messages on page 177](#)

RADIUS IETF Attributes Supported in Disconnect Request Messages

[Table 29 on page 176](#) lists the RADIUS attributes supported by the broadband gateway in Disconnect Request messages.

Table 29: 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

Table 29: RADIUS IETF Attributes Supported in Disconnect Request Messages (*continued*)

Attribute Number	Attribute Name	Description	Content
44	Acct-Session-ID	User Session identifier, unique for every bearer under the session. The broadband gateway deletes 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 Disconnect Request Messages

Table 30 on page 177 lists the 3GPP VSAs supported by the broadband gateway in Disconnect Request messages.

Table 30: 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

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 177](#)
- [3GPP VSAs Supported in CoA Messages on page 178](#)

RADIUS IETF Attributes Supported in CoA Messages

Table 31 on page 178 lists the RADIUS attributes supported by the broadband gateway in CoA messages.

Table 31: 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
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 32 on page 178](#) lists the 3GPP vendor-specific attributes (VSAs) supported by the broadband gateway in CoA messages.

Table 32: 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

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 179.](#)
2. Configure one or more network elements.
See [“Configuring Network Elements” on page 182.](#)
3. (Optional) Configure a network element group to use with accounting.
See [“Configuring Network Element Groups” on page 183.](#)
4. Configure an AAA profile.
See [“Configuring an AAA Profile” on page 184.](#)
5. Configure AAA services for an APN.
See [“Applying an AAA Profile to an APN” on page 190.](#)



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 148](#)
- [Network Elements on page 151](#)
- [Network Element Groups on page 152](#)
- [AAA Profiles on page 153](#)
- [Mobility Maintenance Mode Overview on page 394](#)
- [Modifying an Access Point Name on page 398](#)

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 148](#)
- [Example: Configuring AAA on the Broadband Gateway on page 192](#)

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.
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 allow-dynamic-requests
```

```
[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 148](#)
- [Example: Configuring AAA on the Broadband Gateway on page 192](#)

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 148](#)
- [Example: Configuring AAA on the Broadband Gateway on page 192](#)

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 151](#)
- [Network Element Groups on page 152](#)
- [Example: Configuring AAA on the Broadband Gateway on page 192](#)

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 152](#)
- [Network Elements on page 151](#)
- [Example: Configuring AAA on the Broadband Gateway on page 192](#)

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 184](#).

3. Configure accounting settings for the AAA profile.

See [“Configuring Accounting Settings in an AAA Profile” on page 185](#).

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 186](#).

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 190](#).

Related Documentation

- [Overview of AAA on the Broadband Gateway on page 148](#)
- [AAA Profiles on page 153](#)
- [Example: Configuring AAA on the Broadband Gateway on page 192](#)

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 153](#)
- [Network Elements on page 151](#)
- [Example: Configuring AAA on the Broadband Gateway on page 192](#)

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 33 on page 185](#) 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 33 on page 185](#) lists the events you can specify.

```
[edit unified-edge aaa mobile-profiles aaaprofile radius accounting trigger]
user@host# set trigger no-rat-change
```

Table 33: 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

Table 33: Events You Can Exclude from Triggering Interim-Update Messages (*continued*)

Event	CLI Entry to disable Interim-Updates for the event
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 148](#)
- [AAA Profiles on page 153](#)
- [Network Elements on page 151](#)
- [Network Element Groups on page 152](#)
- [Example: Configuring AAA on the Broadband Gateway on page 192](#)

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 34 on page 187](#) 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 35 on page 187](#) for the RADIUS attributes and message type combinations you can configure. See [Table 36 on page 188](#) 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 36 on page 188](#) 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 34 on page 187](#) lists the attributes supported in the **ignore** statement.

Table 34: RADIUS Attributes the Broadband Gateway Can Ignore in Accept-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 35 on page 187](#) lists the RADIUS attributes and message types supported in the **exclude** statement.

Table 35: 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

Table 35: RADIUS Attributes the Broadband Gateway Can Exclude from RADIUS Messages (*continued*)

CLI Entry	Attribute Name	Attribute Number	Supported Message Type
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
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 36 on page 188](#) 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 36: 3GPP VSAs That Can Be Excluded from RADIUS Messages

CLI Entry	Attribute Name	Attribute Number	Supported Message Type
imei	3GPP-IMEISV	3GPP VSA 26–20	Access-Request Accounting-Start

Table 36: 3GPP VSAs That Can Be Excluded from RADIUS Messages (*continued*)

CLI Entry	Attribute Name	Attribute Number	Supported Message Type
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
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 148](#)
- [AAA Profiles on page 153](#)
- [Example: Configuring AAA on the Broadband Gateway on page 192](#)

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 153](#)
- [Example: Configuring AAA on the Broadband Gateway on page 192](#)

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 105](#)
 - [AAA Profiles on page 153](#)
 - [Example: Configuring AAA on the Broadband Gateway on page 192](#)

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 115](#)
 - [Example: Configuring AAA on the Broadband Gateway on page 192](#)

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 115](#)
 - [Example: Configuring AAA on the Broadband Gateway on page 192](#)

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 148](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 109](#)

Example: Configuring AAA on the Broadband Gateway

- [Requirements on page 192](#)
- [Overview on page 192](#)
- [Configuration on page 195](#)
- [Verification on page 203](#)

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 *imagio*, 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, then the username and password configured under **anonymous-user** are used to authenticate the subscriber.

Configuration

- [Configuring the RADIUS Servers on page 195](#)
- [Configuring the Loopback Interface on page 198](#)
- [Configuring the Network Elements on page 199](#)
- [Configuring the Network Element Group on page 200](#)
- [Configuring the AAA Profile on page 200](#)
- [Applying AAA Services to an APN on page 202](#)

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 trigger interim-interval 10
set unified-edge aaa mobile-profiles aaa-prof radius trigger no-qos-change
set unified-edge aaa mobile-profiles aaa-prof radius options nas-identifier-prefix imagio
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 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 trigger
no-qos-change
```

5. Configure the broadband gateway to set the NAS-Identifier attribute in RADIUS messages to the string *imagio*, 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 imagio
```

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 anonymous-user
  user-name aaa
set unified-edge gateways ggsn-pgw MBG1 apn-services apns internet123 anonymous-user
  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
  anonymous-user user-name aaa
user@pe1# set unified-edge gateways ggsn-pgw MBG1 apn-services apns internet123
  anonymous-user 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 148](#)
 - [Configuring AAA on the Broadband Gateway on page 179](#)
 - [Configuring APNs on the MobileNext Broadband Gateway Overview on page 105](#)
 - [Configuring Anonymous Users on a Broadband Gateway APN on page 114](#)
 - [Configuring Address Assignment on a Broadband Gateway APN on page 115](#)

CHAPTER 8

Configuring DHCP

- [DHCP Overview on page 207](#)
- [DHCP Proxy Client on page 208](#)
- [Configuring DHCP Proxy Client on page 208](#)
- [Configuring DHCP Under APN on page 209](#)

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 systems connected to IP networks must be configured before they can communicate with other computers on the network. DHCP maintains a database that helps to track computers that have been connected to the network and this prevents two computers from accidentally being configured with the same IP address.

The IP address is the most important configuration parameter of the DHCP. A computer must be initially assigned a specific IP address that is appropriate to the network to which the computer is attached and that is not assigned to any other computer on that network. If you move a computer to a new network, it must be assigned a new IP address for that new network. You can use the DHCP to manage these assignments automatically.

An IP 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 MX router to support the following DHCP features:

- DHCP Configuration under APN Configuration
- DHCP Profile Configuration

DHCP Protocol

The DHCP is based on a bootstrap protocol (BOOTP) that provides clients the means to allot their own IP address, the IP address of a server host, and the name of a bootstrap file. DHCP servers can serve requests from BOOTP clients and provide additional capabilities beyond BOOTP, such as the automatic allocation of reusable IP addresses and additional configuration options.

DHCP provides two primary functions:

- Allocating temporary or permanent IP addresses to clients
- Storing, managing, and providing client configuration parameters

DHCP Proxy Client

In regular DHCP client configuration, the client and server are on the same subnet. The client makes a request to the server for an IP address and other configuration items and associates them with the local host interface. This may happen at boot time or at renewal time or at interface initialization. In a DHCP proxy configuration, the client and server are on different subnets. The proxy intercepts the request from the client and mimics the server. It forwards the request from the client to the server and informs the server of the subnet from which the client is requesting an IP address. The server responds with the IP address and other attributes, which are forwarded to the client via the proxy. In a DHCP proxy client, the subscriber manager requests the DHCP server for an IP address and other configurations on behalf of the subscriber. The proxy hides the server details by acting as the server from the view of the subscriber, whereas the actual client uses the IP address and other configuration details. The server notices this proxy agent and communicates to the client like it would communicate with the normal proxy agent in the network.

Configuring DHCP Proxy Client

To configure a DHCPv4 or a DHCPv6 profile, configure the DHCP proxy client on the system services for the routing instance. Use the following procedure to set up a DHCPv4 profile. Use the same procedure to set up a DHCPv6 profile.

To configure a DHCPv4 profile on the system services for a routing instance on an MX router.

1. Configure the bind interfaces for the DHCPv4 profile. For a DHCPv4 proxy client, the interface must be configured with the valid **inet** address and **inet** address family. Similarly, for the DHCPv6 profile, the interface must be configured with the valid **inet6** address and **inet6** family.

```
[edit routing-instances name system services dhcp-proxy-client dhcpv4-profiles name]  
user@host# set bind-interfaces interface-name ip-address
```

2. Configure the dead server retry interval for the DHCPv4 profile. The range for the number of seconds before reconnecting to a dead server, which was marked down in previous attempts, is from 300 through 3600.

```
[edit routing-instances name system services dhcp-proxy-client dhcpv4-profiles name]  
user@host# set dead-server-retry-interval n
```

3. Configure the dead server successive retry attempt for the DHCPv4 profile. The range for the number of successive retry attempts before declaring an unresponsive server dead is from 5 through 1000.

```
[edit routing-instances name system services dhcp-proxy-client dhcpv4-profiles name]  
user@host# set dead-server-successive-retry-attempt n
```

4. Configure the DHCP server selection algorithm for the DHCPv4 profile. The DHCP server is selected either by the highest priority or round-robin method, according to the option specified for server selection.

```
[edit routing-instances name system services dhcp-proxy-client dhcpv4-profiles name]
user@host# set dhcp-server-selection-algorithm [highest-priority-server | round-robin]
```

5. Configure the lease time for the DHCPv4 profile. The range for the minimum and maximum allowable lease times that are accepted in responses from DHCP servers is from 60 through 1000.

```
[edit routing-instances name system services dhcp-proxy-client dhcpv4-profiles name]
user@host# set lease-time n
```

6. Configure the pool name for the DHCPv4 profile. The pool name is sent to the server only if it is configured and is optional.

```
[edit routing-instances name system services dhcp-proxy-client dhcpv4-profiles name]
user@host# set pool-name string
```

7. Configure the retransmission attempt for the DHCPv4 profile. The range for the maximum number of times that the system attempts to communicate with the unresponsive DHCP server before it is considered a failure is from 0 through 1000.

```
[edit routing-instances name system services dhcp-proxy-client dhcpv4-profiles name]
user@host# set retransmission-attempt n
```

8. Configure the retransmission interval for the DHCPv4 profile. The range for the amount of time that must pass with no response before the system reattempts to communicate with the DHCP server is from 4 through 64.

```
[edit routing-instances name system services dhcp-proxy-client dhcpv4-profiles name]
user@host# set retransmission-interval n
```

9. Configure the servers for the DHCPv4 profile. This is applicable only to DHCPv4 and a minimum of one server must be configured for effective communication between the DHCP proxy clients and the DHCP server.

```
[edit routing-instances name system services dhcp-proxy-client dhcpv4-profiles name]
user@host# set servers ip-v4address priority;
```

Configuring DHCP Under APN

To configure a DHCPv4-proxy-client-profile or a DHCPv6-proxy-client-profile, configure the address assignment on the APN services for **unified-edge gateways ggsn-pgw**. Use the following configuration to set up a DHCPv4-proxy client profile. Use the same procedures to set up a DHCPv6-proxy client profile.

To configure a DHCPv4 profile on the system services for a routing instance on an MX router:

1. Configure the DHCPv4 proxy client profile.

```
[edit unified-edge gateways ggsn-pgw name apn-services apn name
address-assignment]
user@host# set dhcpv4-proxy-client-profile logical-system ls routing-instance ri
profile-name dhcpv4-prof-name name-of-pool-to-send-to-dhcp-server
```


PART 5

GPRS Tunneling Protocol (GTP) Configuration

- [Configuring GTP on page 213](#)

CHAPTER 9

Configuring GTP

- [GTP Versions and GPRS Interfaces Overview on page 214](#)
- [GPRS Tunneling Protocol \(GTP\) Overview on page 216](#)
- [GTP Path Management Overview on page 216](#)
- [Understanding Path Management on page 218](#)
- [GTP Tunnel Management Overview on page 220](#)
- [Understanding Tunnel Management on page 221](#)
- [Restart Counters Overview on page 223](#)
- [Understanding CSID Signaling on page 224](#)
- [Understanding Tunnel Endpoint Identifiers on page 225](#)
- [Configuring GTP Services Overview on page 226](#)
- [Configuring a Loopback Interface for Transport of GTP Packets on page 228](#)
- [Configuring GTP Services on a Broadband Gateway on page 229](#)
- [Configuring GTP Services on the Control Plane on page 230](#)
- [Configuring GTP Services on the Data Plane on page 232](#)
- [Configuring GTP Services on the S5 Interface on page 233](#)
- [Configuring GTP Services on the S8 Interface on page 235](#)
- [Configuring GTP Services on the Gn Interface on page 236](#)
- [Configuring GTP Services on the Gp Interface on page 238](#)
- [Configuring GTP Services When the S5 and S8 Interfaces Are in Different VRFs on page 239](#)
- [Configuring GTP Services When the S5 and S8 Interfaces Are in the Same VRF on page 241](#)
- [Configuring GTP Services When 3GPP Interfaces Are in Different VRFs on page 242](#)
- [Configuring GTP Services on a GGSN Broadband Gateway on page 244](#)
- [Configuring GTP Services on a Peer Group on page 245](#)
- [Disabling Path Management on a Broadband Gateway or Peer Group on page 247](#)
- [Configuring GTP Trace Options on page 247](#)
- [Configuring General GTP Service on the S-GW on page 249](#)

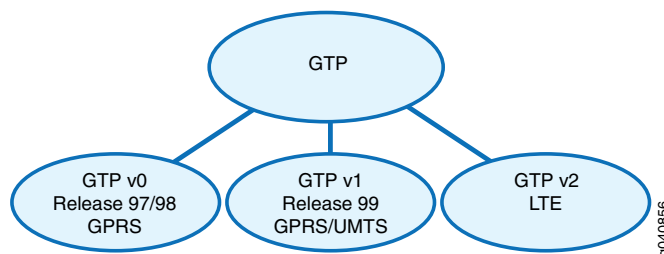
- [Configuring GTP-C Services on the S11 Interface on page 252](#)
- [Configuring GTP-U Services on the S12 Interface on page 254](#)
- [Configuring GTP Services on the S1-U Interface on page 256](#)
- [Configuring GTP Services on the S4 Interface on page 257](#)
- [Configuring GTP Services on the S-GW When the S4 and S5 Interfaces Are in the Same VRF on page 259](#)
- [Configuring GTP Services on the S-GW When Interfaces are in Different VRFs on page 261](#)
- [Configuring S-GW GTP Traceoptions on page 262](#)
- [Example: Configuring GTP for the S-GW When Interfaces Are in different VRFs on page 265](#)

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 34 on page 214](#) shows the GTP versions that the broadband gateway supports.

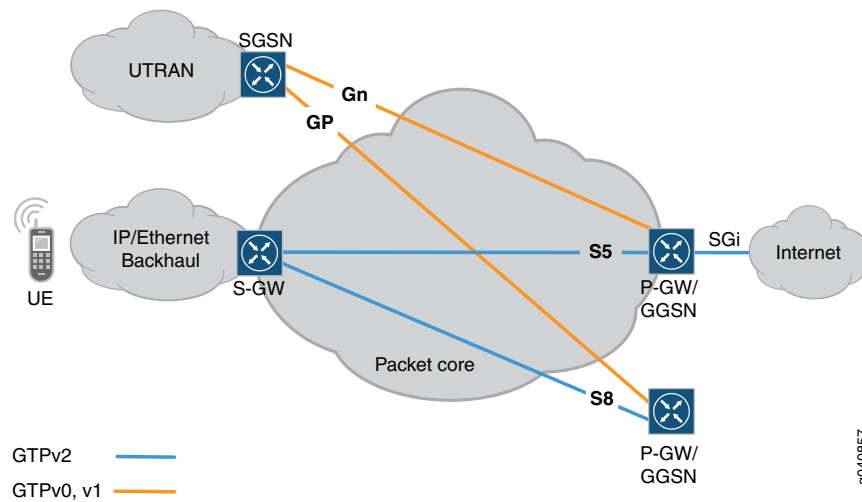
Figure 34: GTP Versions Supported on a MobileNext Broadband Gateway



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 35 on page 215](#) shows the GTP-C versions the broadband gateway supports for the 3G and 4G network interfaces.

Figure 35: GTP-C Versions Supported for 3G/4G Network Interfaces



For 3G networks, a broadband gateway uses GTP v0, or GTPv, 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 216](#)
- [GTP Tunnel Management Overview on page 220](#)
- [Configuring General GTP Service on the S-GW on page 249](#)

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 226](#)
- [GTP Path Management Overview on page 216](#)
- [GTP Tunnel Management Overview on page 220](#)
- [Configuring General GTP Service on the S-GW on page 249](#)

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 217](#)
- [GTP Version Support for Echo Requests and Echo Responses on page 217](#)

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 226](#)
- [GTP Tunnel Management Overview on page 220](#)
- [Understanding Tunnel Endpoint Identifiers on page 225](#)
- [Configuring General GTP Service on the S-GW on page 249](#)

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.

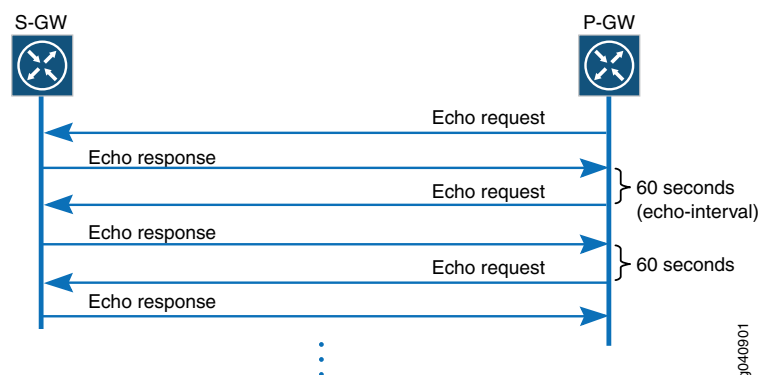
This topic includes the following sections:

- [Successful Echo-Request Sequence for Path Management on page 218](#)
- [Failed Echo Request Sequence for Path Management on page 219](#)

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 36 on page 218](#) shows a successful echo-request sequence, in which the P-GW receives an echo response for each echo request.

Figure 36: Successful Echo-Request Sequence for Path Management



The following steps describe the echo request/response sequence in [Figure 36 on page 218](#):

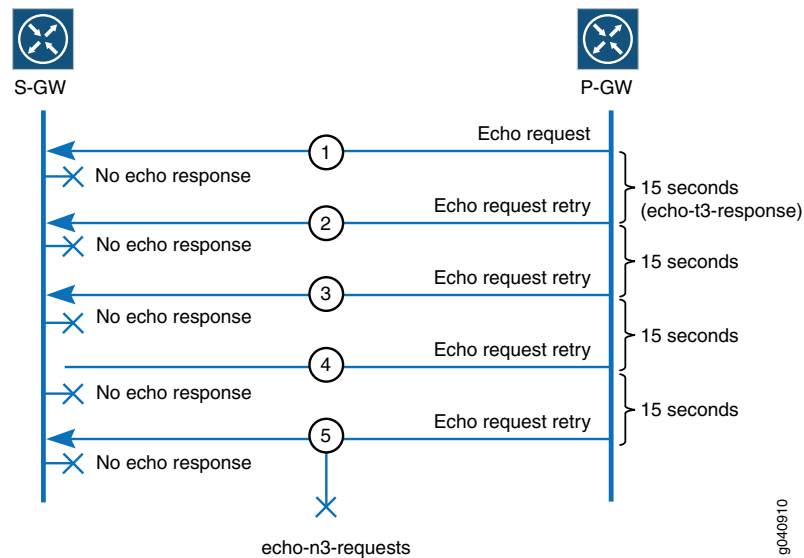
1. An echo request is sent, and the P-GW receives an echo response within the specified **echo-t3-response** time.
2. The P-GW waits for the configured echo-interval (or default echo-interval of 60 seconds) before sending another echo request, and the P-GW receives an echo response within the specified **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 37 on page 219](#) 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 37: Failed Echo-Request Sequence for Path Management



The following steps describe the echo-request and echo-response sequence in [Figure 37 on page 219](#):

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 226](#)
 - [GTP Path Management Overview on page 216](#)
 - [GTP Tunnel Management Overview on page 220](#)
 - [Understanding Tunnel Endpoint Identifiers on page 225](#)
 - [Configuring General GTP Service on the S-GW on page 249](#)

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 220](#)
- [Default Tunnel Management Configuration on page 220](#)
- [GTP Version Support for Tunnel Management Requests and Responses on page 220](#)

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 226](#)
- [GTP Path Management Overview on page 216](#)
- [Understanding Tunnel Endpoint Identifiers on page 225](#)
- [Configuring General GTP Service on the S-GW on page 249](#)

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 221](#)
- [Successful Update/Delete Request Sequence for Tunnel Management on page 222](#)
- [Failed Update/Delete Request Sequence for Tunnel Management on page 222](#)

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 38 on page 221](#) shows a successful Create request sequence in which the S-GW receives a response after sending a request.

Figure 38: Successful Create Request Sequence for Tunnel Management



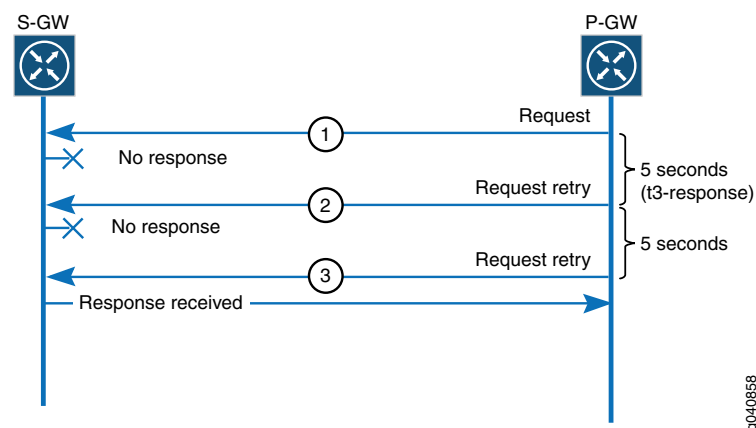
The following steps describe the tunnel management Create request sequence in [Figure 38 on page 221](#):

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 39 on page 222](#) 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 39: Successful Update/Delete Request Sequence for Tunnel Management



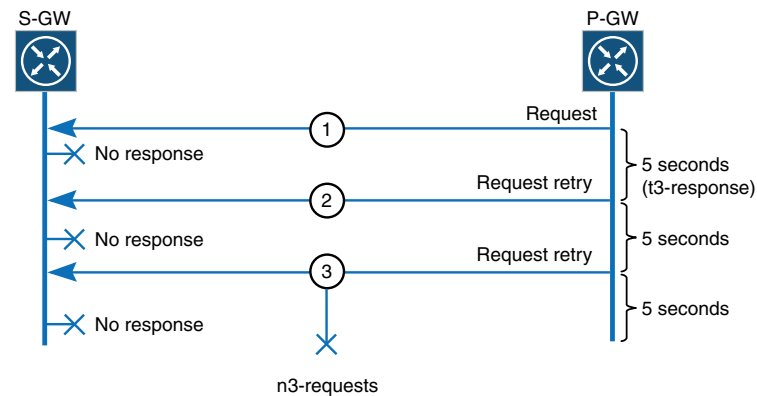
The following steps describe the tunnel management Update or Delete request sequence in [Figure 39 on page 222](#):

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 40 on page 223](#) 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 40: Failed Update/Delete Request Sequence for Tunnel Management



g040900

The following steps describe the Update or Delete request failed sequence in [Figure 40 on page 223](#):

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 226](#)
- [GTP Path Management Overview on page 216](#)
- [GTP Tunnel Management Overview on page 220](#)
- [Understanding Tunnel Endpoint Identifiers on page 225](#)
- [Configuring General GTP Service on the S-GW on page 249](#)

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 226](#)
- [GTP Path Management Overview on page 216](#)
- [GTP Tunnel Management Overview on page 220](#)
- [Configuring General GTP Service on the S-GW on page 249](#)

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 216](#)
- [GTP Path Management Overview on page 216](#)
- [GTP Tunnel Management Overview on page 220](#)
- [Understanding Tunnel Endpoint Identifiers on page 225](#)

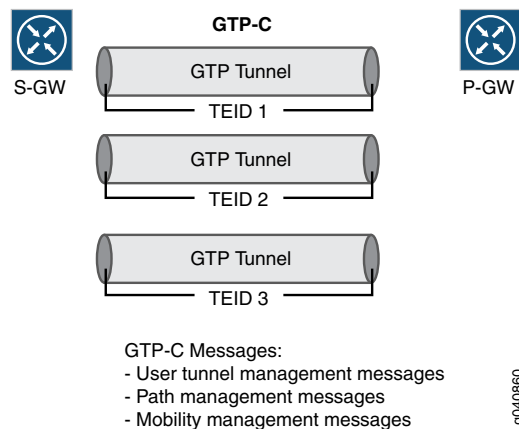
- [Configuring General GTP Service on the S-GW on page 249](#)

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 41 on page 225](#) shows a GTP tunnel with its associated TEID.

Figure 41: 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 41 on page 225](#). 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)

Each GTP-U tunnel is also assigned a TEID. For example, the GTP-U tunnel for a default bearer would have its own TEID.

- Related Documentation**
- [Configuring GTP Services Overview on page 226](#)
 - [GTP Path Management Overview on page 216](#)
 - [GTP Tunnel Management Overview on page 220](#)
 - [Configuring General GTP Service on the S-GW on page 249](#)

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 226](#)
- [Configuring GTP Services at Different Levels on a Broadband Gateway on page 226](#)
- [GTP Services Default Settings on page 227](#)
- [GTP Version Support on page 228](#)

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 216](#).

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 220](#).

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 216](#)
- [GTP Path Management Overview on page 216](#)
- [GTP Tunnel Management Overview on page 220](#)
- [Configuring General GTP Service on the S-GW on page 249](#)

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 229](#)
- [Configuring General GTP Service on the S-GW on page 249](#)

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 228](#)
- [Configuring GTP Services on the Data Plane on page 232](#)
 - [Configuring GTP Services on the Control Plane on page 230](#)
- [Configuring GTP Services Overview on page 226](#)
- [Configuring General GTP Service on the S-GW on page 249](#)

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 228](#)
- [Configuring GTP Services on the Data Plane on page 232](#)
- [Configuring GTP Services on a Broadband Gateway on page 229](#)
- [Configuring GTP Services Overview on page 226](#)
- [Configuring General GTP Service on the S-GW on page 249](#)

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 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 data]
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 data]
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 data]
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 data]
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 data]
user@host# set echo-interval 65
```

7. 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 225](#)
 - [Configuring a Loopback Interface for Transport of GTP Packets on page 228](#)
 - [Configuring GTP Services on the Control Plane on page 230](#)
 - [Configuring GTP Services on a Broadband Gateway on page 229](#)
 - [Configuring GTP Services Overview on page 226](#)
 - [Configuring General GTP Service on the S-GW on page 249](#)

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 228](#)
- [Configuring GTP Services on the S8 Interface on page 235](#)
- [Configuring GTP Services on the Data Plane on page 232](#)
- [Configuring GTP Services on the Control Plane on page 230](#)
- [Configuring GTP Services on a Broadband Gateway on page 229](#)
- [Configuring GTP Services Overview on page 226](#)
- [Configuring General GTP Service on the S-GW on page 249](#)

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 228](#)
- [Configuring GTP Services on the S5 Interface on page 233](#)
- [Configuring GTP Services on the Data Plane on page 232](#)
- [Configuring GTP Services on the Control Plane on page 230](#)
- [Configuring GTP Services on a Broadband Gateway on page 229](#)
- [Configuring GTP Services Overview on page 226](#)
- [Configuring General GTP Service on the S-GW on page 249](#)

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 228](#)
- [Configuring GTP Services on the Gp Interface on page 238](#)
- [Configuring GTP Services on the Data Plane on page 232](#)
- [Configuring GTP Services on the Control Plane on page 230](#)
- [Configuring GTP Services on a Broadband Gateway on page 229](#)
- [Configuring GTP Services Overview on page 226](#)
- [Configuring General GTP Service on the S-GW on page 249](#)

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 228](#)
- [Configuring GTP Services on the Gn Interface on page 236](#)
- [Configuring GTP Services on the Data Plane on page 232](#)
- [Configuring GTP Services on the Control Plane on page 230](#)
- [Configuring GTP Services on a Broadband Gateway on page 229](#)
- [Configuring GTP Services Overview on page 226](#)
- [Configuring General GTP Service on the S-GW on page 249](#)

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 228](#)
- [Configuring GTP Services on the Data Plane on page 232](#)
- [Configuring GTP Services on the Control Plane on page 230](#)

- [Configuring GTP Services on a Broadband Gateway on page 229](#)
- [Configuring GTP Services Overview on page 226](#)
- [Configuring General GTP Service on the S-GW on page 249](#)

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 228](#)
- [Configuring GTP Services on the Data Plane on page 232](#)
- [Configuring GTP Services on the Control Plane on page 230](#)
- [Configuring GTP Services on a Broadband Gateway on page 229](#)
- [Configuring GTP Services Overview on page 226](#)
- [Configuring General GTP Service on the S-GW on page 249](#)

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 228](#)
- [Configuring GTP Services on the Data Plane on page 232](#)
- [Configuring GTP Services on the Control Plane on page 230](#)
- [Configuring GTP Services on a Broadband Gateway on page 229](#)
- [Configuring GTP Services Overview on page 226](#)
- [Configuring General GTP Service on the S-GW on page 249](#)

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 228](#)
- [Configuring GTP Services Overview on page 226](#)
- [Configuring GTP Services on the Data Plane on page 232](#)
- [Configuring GTP Services on the Control Plane on page 230](#)
- [Configuring GTP Services on a Broadband Gateway on page 229](#)
- [Configuring GTP Services When 3GPP Interfaces Are in Different VRFs on page 242](#)
- [Configuring General GTP Service on the S-GW on page 249](#)

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 228](#)
- [Configuring GTP Services on the Data Plane on page 232](#)
- [Configuring GTP Services on the Control Plane on page 230](#)
- [Configuring GTP Services on a Broadband Gateway on page 229](#)
- [Configuring GTP Services Overview on page 226](#)
- [Configuring General GTP Service on the S-GW on page 249](#)

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 216](#)
- [Configuring GTP Services Overview on page 226](#)
- [Configuring General GTP Service on the S-GW on page 249](#)

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 37 on page 247](#) describes the flags that you can include.

Table 37: Trace Flags

Flag	Description
all	Trace everything.
config	Trace configuration-related information.
debug	Trace debug information.

Table 37: Trace Flags (*continued*)

decode	Trace decoding of received packets.
encode	Trace encoding of transmitted packets.
events	Trace all internal and external events.
packet-io	Trace transmitted and received packets.
peer	Trace decoding of received packets.
tracker	Trace GTP peer-related events.
warning	Trace warnings.

[Table 38 on page 248](#) describes the levels you can include.

Table 38: Trace Levels

Level	Description
all	Match all levels.
error	Match error conditions.
info	Match informational messages.
notice	Match conditions that should be specially handled.
verbose	Match verbose messages.
warning	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 226](#)
- [Configuring General GTP Service on the S-GW on page 249](#)

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 216](#)
- [Configuring GTP Services on the S4 Interface on page 257](#)
- [Configuring GTP-C Services on the S11 Interface on page 252](#)
- [Configuring GTP-U Services on the S12 Interface on page 254](#)
- [Configuring GTP Services on the S1-U Interface on page 256](#)
- [Example: Configuring GTP for the S-GW When Interfaces Are in different VRFs on page 265](#)

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 216](#)
- [Configuring General GTP Service on the S-GW on page 249](#)
- [Configuring GTP Services on the S4 Interface on page 257](#)
- [Configuring GTP-U Services on the S12 Interface on page 254](#)
- [Configuring GTP Services on the S1-U Interface on page 256](#)
- [Example: Configuring GTP for the S-GW When Interfaces Are in different VRFs on page 265](#)

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 216](#)
- [Configuring General GTP Service on the S-GW on page 249](#)
- [Configuring GTP Services on the S4 Interface on page 257](#)
- [Configuring GTP-C Services on the S11 Interface on page 252](#)
- [Configuring GTP Services on the S1-U Interface on page 256](#)
- [Example: Configuring GTP for the S-GW When Interfaces Are in different VRFs on page 265](#)

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 216](#)
- [Configuring General GTP Service on the S-GW on page 249](#)
- [Configuring GTP Services on the S4 Interface on page 257](#)
- [Configuring GTP-C Services on the S11 Interface on page 252](#)
- [Configuring GTP-U Services on the S12 Interface on page 254](#)
- [Example: Configuring GTP for the S-GW When Interfaces Are in different VRFs on page 265](#)

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 216](#)
- [Configuring General GTP Service on the S-GW on page 249](#)
- [Configuring GTP-C Services on the S11 Interface on page 252](#)
- [Configuring GTP-U Services on the S12 Interface on page 254](#)
- [Example: Configuring GTP for the S-GW When Interfaces Are in different VRFs on page 265](#)

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 249](#)
- [Configuring GTP Services on the S4 Interface on page 257](#)

- [Configuring GTP Services on the S5 Interface on page 233](#)
- [Configuring GTP Services on the S-GW When the S4 and S5 Interfaces Are in the Same VRF on page 259](#)
- [GPRS Tunneling Protocol \(GTP\) Overview on page 216](#)

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:
- 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
```

- 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 249](#)
- [Configuring GTP Services on the S4 Interface on page 257](#)
- [Configuring GTP Services on the S5 Interface on page 233](#)
- [Configuring General GTP Service on the S-GW on page 249](#)
- [Configuring GTP Trace Options on page 247](#)
- [Configuring S-GW GTP Traceoptions on page 262](#)
- [GPRS Tunneling Protocol \(GTP\) Overview on page 216](#)

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 39 on page 263](#) 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 39: S-GW GTP Trace Flags

Flag	Description
all	Trace everything.
config	Trace configuration events.
debug	Trace debug information
decode	Trace decoding of received packets.
encode	Trace encoding of transmitted packets.
error	Trace internal or external errors.
events	Trace all internal or external events.
packet-io	Trace transmitted and received packets.
peer	Trace GTP peer-related events.
trackers	Trace GTP tracker-related events.
warning	Trace warnings.

Table 40 on page 263 describes the levels you can include.

Table 40: S-GW GTP Trace Levels

Level	Description
all	Match all levels.
error	Match error conditions.
info	Match informational messages.
notice	Match conditions that should be specially handled.
verbose	Match verbose messages.
warning	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 249](#)
- [Configuring GTP Trace Options on page 247](#)
- [GPRS Tunneling Protocol \(GTP\) Overview on page 216](#)
- [Configuring S-GW Traceoptions on page 33](#)
- [Configuring S-GW Data Path Traceoptions on page 97](#)
- [Configuring S-GW Charging Traceoptions on page 284](#)
- [Configuring S-GW Local Persistent Storage Traceoptions on page 287](#)

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 265](#)
- [Overview on page 265](#)
- [Configuration on page 265](#)

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 41: Components of the Broadband Gateway

Property	Settings	Description
Loopback addresses	lo0 unit 111 address 192.168.111.1/32 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 lo0.111	VRF for S11/S5 interfaces for control
S1-U/S12/S4/S5 data connectivity	VRF12-Data lo0.122	VRF for S1-U/S12/S4 interfaces for data

Configuration

- [Configuring the Interfaces on page 266](#)
- [Enabling the Routing Instances for the VRF on page 267](#)

- [Configuring GTP Interfaces on page 268](#)
- [\[xref target has no title\]](#)

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 249](#)
 - [Configuring GTP Trace Options on page 247](#)
 - [GPRS Tunneling Protocol \(GTP\) Overview on page 216](#)

PART 6

Charging Configuration

- [Charging Overview on page 271](#)
- [Configuring Charging on page 279](#)

CHAPTER 10

Charging Overview

- [Charging on page 271](#)
- [Charging Services Overview on page 271](#)
- [Charging Data Records on page 273](#)
- [Charging Profiles on page 277](#)

Charging

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 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.

The broadband gateway provides support for billing through offline charging, RADIUS accounting, or both. RADIUS accounting delivers accounting information used for billing to the RADIUS accounting server.

Related Documentation

- [Charging Services Overview on page 271](#)

Charging Services 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

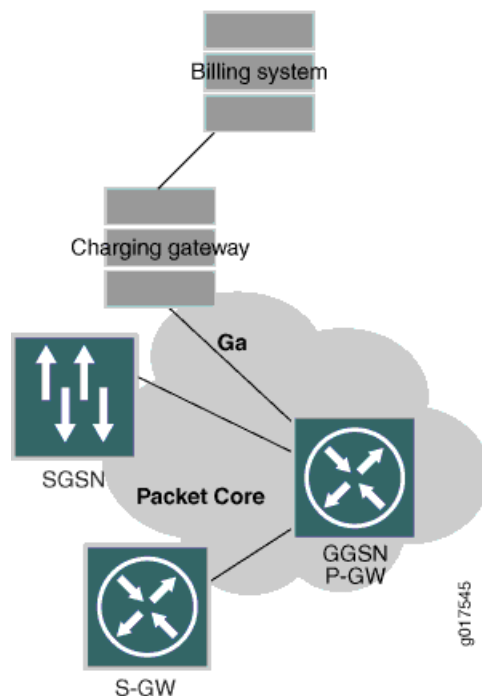
record collection for their mobile subscribers. The broadband gateway gathers Charging Data Records (CDRs) and delivers them to the charging gateway function (CGF) over the Ga interface using the GTP Prime protocol. The billing function is distributed across all modules of the broadband gateway, which performs these tasks for billing:

- Accurate CDR creation and closure
- Partial record generation
- ASN.1 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 42 on page 272 shows the components in a sample charging topology.

Figure 42: 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 AVP 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

- [Configuring GTP Prime for Charging on page 289](#)
- [Configuring Persistent Storage on page 291](#)
- [Charging Data Records on page 273](#)
- [Charging Profiles on page 277](#)

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 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***_***RC***.***date***_***time***[***.PI***].cdr, where:

- *NodeID*—Name of the host that generated the file.
- *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*.

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

- [Configuring Charging on page 279](#)
- [Configuring Transport Profiles on page 295](#)

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**

- [Configuring Charging Profiles on page 300](#)
- [Configuring Transport Profiles on page 295](#)
- [Configuring Charging Trigger Events on page 296](#)
- [Configuring CDR Attributes on page 298](#)
- [Configuring Charging Profiles for APNs on page 301](#)

Configuring Charging

- [Configuring Charging on page 279](#)
- [Configuring S-GW-Specific Charging Parameters on page 280](#)
- [Configuring S-GW Global Charging Profiles and Selection Order on page 282](#)
- [Configuring S-GW Charging Traceoptions on page 284](#)
- [Configuring S-GW Local Persistent Storage Traceoptions on page 287](#)
- [Configuring GTP Prime for Charging on page 289](#)
- [Configuring Persistent Storage on page 291](#)
- [Configuring the Solid State Disk for Persistent Storage on page 293](#)
- [Configuring Transport Profiles on page 295](#)
- [Configuring Charging Trigger Events on page 296](#)
- [Configuring CDR Attributes on page 298](#)
- [Configuring Charging Profiles on page 300](#)
- [Configuring Charging Profiles for APNs on page 301](#)
- [Tracing Charging Operations on page 302](#)
- [Verifying and Managing the Charging Configuration on page 304](#)

Configuring 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 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 do not configure the GTP Prime properties for the 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 289](#)
- [Configuring Persistent Storage on page 291](#)
- [Configuring Transport Profiles on page 295](#)
- [Configuring Charging Trigger Events on page 296](#)
- [Configuring CDR Attributes on page 298](#)
- [Configuring Charging Profiles on page 300](#)
- [Configuring Charging Profiles for APNs on page 301](#)
- [Tracing Charging Operations on page 302](#)
- [Charging Data Records on page 273](#)

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 a 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 exclude 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]
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 information element.

```
[edit unified-edge gateways sgw MBG-SGW1 charging cdr-profiles CDR1
exclude-ie-options]
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 information element.

```
[edit unified-edge gateways sgw MBG-SGW1 charging cdr-profiles CDR1
exclude-ie-options]
user@host# set sgw-change
```



NOTE: When this statement is configured, the S-GW change information element 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 support Release 8. You must include this statement to change the supported release.

Related Documentation

- [Configuring Charging on page 279](#)
- [Configuring S-GW Global Charging Profiles and Selection Order on page 282](#)
- [Configuring S-GW Charging Traceoptions on page 284](#)
- [Configuring S-GW Local Persistent Storage Traceoptions on page 287](#)
- [Configuring GTP Prime for Transferring CDRs on page 289](#)
- [Configuring Persistent Storage on page 291](#)
- [Configuring Transport Profiles on page 295](#)
- [Configuring Charging Trigger Events on page 296](#)
- [Configuring CDR Attributes on page 298](#)

- [Configuring Charging Profiles on page 300](#)
- [Configuring Charging Profiles for APNs on page 301](#)
- [Tracing Charging Operations on page 302](#)
- [Charging Data Records on page 273](#)

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 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 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 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 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 Charging on page 279](#)
- [Configuring S-GW-Specific Charging Parameters on page 280](#)
- [Configuring S-GW Charging Traceoptions on page 284](#)
- [Configuring S-GW Local Persistent Storage Traceoptions on page 287](#)

- [Configuring GTP Prime for Transferring CDRs on page 289](#)
- [Configuring Persistent Storage on page 291](#)
- [Configuring Transport Profiles on page 295](#)
- [Configuring Charging Trigger Events on page 296](#)
- [Configuring CDR Attributes on page 298](#)
- [Configuring Charging Profiles on page 300](#)
- [Configuring Charging Profiles for APNs on page 301](#)
- [Tracing Charging Operations on page 302](#)
- [Charging Data Records on page 273](#)

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 42 on page 284](#) 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 42: S-GW Charging Trace Flags

Flag	Description
all	Trace everything.
cdr-encoding	Trace Charging Detail Record (CDR) encoding.
client-fsm	Trace client finite state machine (FSM).
config	Trace configuration events.
fsm	Trace FSM events.
general	Trace general events.
group-fsm	Trace group FSM events.
init	Trace initialization events.
ipc	Trace IPC events.
path-management	Trace path management module.
request	Trace requests.

Table 42: S-GW Charging Trace Flags (*continued*)

resource	Trace resources.
response	Trace response.
timers	Trace timers.
transport	Trace transport group.
triggers	Trace trigger information.

Table 43 on page 285 describes the levels you can include.

Table 43: S-GW Charging Trace Levels

Level	Description
all	Match all levels.
error	Match error conditions.
info	Match informational messages.
notice	Match conditions that should be specially handled.
verbose	Match verbose messages.
warning	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 Charging on page 279](#)
- [Configuring S-GW-Specific Charging Parameters on page 280](#)
- [Configuring S-GW Global Charging Profiles and Selection Order on page 282](#)
- [Configuring S-GW Local Persistent Storage Traceoptions on page 287](#)
- [Configuring GTP Prime for Transferring CDRs on page 289](#)
- [Configuring Persistent Storage on page 291](#)
- [Configuring Transport Profiles on page 295](#)
- [Configuring Charging Trigger Events on page 296](#)
- [Configuring CDR Attributes on page 298](#)
- [Configuring Charging Profiles on page 300](#)
- [Configuring Charging Profiles for APNs on page 301](#)
- [Tracing Charging Operations on page 302](#)
- [Charging Data Records on page 273](#)
- [Configuring S-GW Traceoptions on page 33](#)
- [Configuring S-GW Data Path Traceoptions on page 97](#)
- [Configuring S-GW GTP Traceoptions on page 262](#)
- [Configuring S-GW Local Persistent Storage Traceoptions on page 287](#)

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 44 on page 287 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 44: S-GW Local Persistent Storage Trace Flags

Flag	Description
all	Trace everything.
connection	Trace connection establishment with peers.
file-operations	Trace file open, write, and close operations.
general	Trace miscellaneous operations.
journaling	Trace file journaling operations.
mirror	Trace mirroring operations.

Table 45 on page 287 describes the levels you can include.

Table 45: S-GW Local Persistent Storage Trace Levels

Level	Description
all	Match all levels.
error	Match error conditions.
info	Match informational messages.
notice	Match conditions that should be specially handled.
verbose	Match verbose messages.
warning	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 Charging on page 279](#)
- [Configuring S-GW-Specific Charging Parameters on page 280](#)
- [Configuring S-GW Global Charging Profiles and Selection Order on page 282](#)
- [Configuring S-GW Charging Traceoptions on page 284](#)
- [Configuring GTP Prime for Transferring CDRs on page 289](#)
- [Configuring Persistent Storage on page 291](#)
- [Configuring Transport Profiles on page 295](#)
- [Configuring Charging Trigger Events on page 296](#)
- [Configuring CDR Attributes on page 298](#)

- [Configuring Charging Profiles on page 300](#)
- [Configuring Charging Profiles for APNs on page 301](#)
- [Tracing Charging Operations on page 302](#)
- [Charging Data Records on page 273](#)
- [Configuring S-GW Traceoptions on page 33](#)
- [Configuring S-GW Data Path Traceoptions on page 97](#)
- [Configuring S-GW GTP Traceoptions on page 262](#)
- [Configuring S-GW Charging Traceoptions on page 284](#)

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 289](#)
- [Configuring GTP Prime Peers on page 290](#)

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 Charging on page 279](#)
 - [Configuring Transport Profiles on page 295](#)
 - [Charging Services Overview on page 271](#)

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 291](#)
- [Tracing Persistent Storage Operations on page 292](#)

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
all	Trace all operations
connection	Trace connection establishment between the Routing Engine and all session DPCs for CDR file backup
file-operations	Trace file operations (open, write, close)

Flag	Description
general	Trace miscellaneous operations
journaling	Trace file journaling operations
mirror	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 293](#)
- [Configuring Charging on page 279](#)
- [Configuring Transport Profiles on page 295](#)
- [Charging Services Overview on page 271](#)
- [Configuring S-GW-Specific Charging Parameters on page 280](#)
- [Configuring S-GW Global Charging Profiles and Selection Order on page 282](#)
- [Configuring S-GW Charging Traceoptions on page 284](#)
- [Configuring S-GW Charging Traceoptions on page 284](#)

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 293](#)
- [Ejecting the Solid State Disk on page 294](#)
- [Installing the Solid State Disk on page 294](#)

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 291](#)
- [request system storage unified-edge charging media start on page 1119](#)
- [request system storage unified-edge charging media stop on page 1120](#)
- [request system storage unified-edge media eject on page 1121](#)
- [request system storage unified-edge media prepare on page 1122](#)

Configuring Transport Profiles

A transport profile provides information for transporting the Charging Data Records (CDRs) from the charging data function (CDF) to the charging gateways or to local persistent storage. A transport profile can be associated with different charging profiles. You can define up to eight transport profiles.

To configure transport profiles:

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
```

2. Specify a description for the profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles profile-name]
user@host# set description string
```

3. Configure offline charging in the transport profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles profile-name]
user@host# edit offline charging-gateways
```

4. 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
```

5. Specify the time 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
```

6. 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
```

7. 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 (r99 | r7 | r8)
```

8. Specify the number of CDRs in one DRT message.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
transport-profile1 offline charging-gateways]
user@host# set cdr-aggregation-limit value
```

9. Configure the maximum transmission unit (MTU) of the DRT message.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging transport-profiles
transport-profile1 offline charging-gateways]
user@host# set mtu value
```

Related Documentation

- [Configuring Charging on page 279](#)
- [Configuring GTP Prime for Charging on page 289](#)
- [Configuring Persistent Storage on page 291](#)
- [Configuring Charging Profiles on page 300](#)
- [Charging Profiles on page 277](#)
- [Configuring S-GW-Specific Charging Parameters on page 280](#)
- [Configuring S-GW Global Charging Profiles and Selection Order on page 282](#)
- [Configuring S-GW Charging Traceoptions on page 284](#)
- [Configuring S-GW Charging Traceoptions on page 284](#)

Configuring Charging Trigger Events

A trigger profile defines the charging events that cause Charging Data Record (CDR) changes.

To configure trigger profiles:

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
```

2. Specify a description for the profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name]
user@host# set description string
```

3. Configure offline charging in the trigger profile.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name]
user@host# edit offline
```

4. Specify a time limit for closing the container. 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
```

5. Specify the bearer information change that does 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
```

The following table describes the bearer information changes that can be ignored for charging data updates.

Bearer Information Change	Description
ms-timezone-change	MS time zone
plmn-change	Public Land Mobile Network (PLMN)
qos-change	Quality of service (QoS)
rat-change	Radio Access Technology (RAT)
sgsn-sgw-change	SGSN or S-GW limit
user-location-change	User location information

For example:

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
offline]
user@host# set exclude user-location-change
```

6. 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
```

7. 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)
```

8. Specify the maximum number of containers to limit for each CDR.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
offline]
```

```
user@host# set container-limit value
```

9. Specify the number of SGSN or S-GW changes that can occur before the CDR is updated and closed. A value of zero (0) disables this trigger.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging trigger-profiles profile-name
offline]
```

```
user@host# set sgsn-sgw-change-limit value
```

10. 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.

```
[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

- [Configuring Charging on page 279](#)
- [Configuring Charging Profiles on page 300](#)
- [Charging Profiles on page 277](#)
- [Configuring S-GW-Specific Charging Parameters on page 280](#)
- [Configuring S-GW Global Charging Profiles and Selection Order on page 282](#)
- [Configuring S-GW Charging Traceoptions on page 284](#)
- [Configuring S-GW Charging Traceoptions on page 284](#)

Configuring CDR Attributes

A Charging Data Record (CDR) profile defines the attributes in each CDR.

To configure CDR profiles:

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
```

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
```

- Set optional information elements to exclude from the CDR. You can specify the excluded information elements so that you can manage the size of the CDR. By default, all informational elements are included in the CDR.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging cdr-profiles profile-name]
user@host# set exclude-ie-options [information element]
```

The following table describes the information elements that can be excluded from CDRs.

Information Element	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
lrsn	Local record sequence number
ms-time-zone	Mobile station (MS) time zone
network-initiation	Network initiation flag
node-id	Node identifier
pdn-connection-id	Packet data network (PDN) connection ID
pdppdn-type	PDP or PDN type
pgw-plmn-identifier	Packet Data Network Gateway (P-GW) Public Land Mobile Network (PLMN) identifier field
rat-type	Radio Access Technology (RAT) type
record-sequence-number	Record sequence number
served-imeisv	Served International Mobile Equipment Identity and Software Version Number (IMEISV)
served-msisdn	Served mobile station ISDN (MSISDN)
served-pdppdn-address	Served PDP context or IP-CAN bearer address

Information Element	Information in CDRs
serving-node-plmn-identifier	Serving node PLMN identifier field
start-time	Time when session established; added to first CDR
stop-time	Time when session terminated; added to last CDR
user-location-information	User location information

Related Documentation

- [Configuring Charging on page 279](#)
- [Configuring Charging Profiles on page 300](#)
- [Charging Profiles on page 277](#)
- [Configuring S-GW-Specific Charging Parameters on page 280](#)
- [Configuring S-GW Global Charging Profiles and Selection Order on page 282](#)
- [Configuring S-GW Charging Traceoptions on page 284](#)
- [Configuring S-GW Charging Traceoptions on page 284](#)

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, a trigger profile, and other default service-aware charging information.

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
```
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 defined.


```
[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
```

- (Optional) Specify the default rating group. This option is useful for the 3GPP Release 8 specifications or for generating a Release 7 service data container.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging charging-profiles profile-name]
user@host# set default-rating-group integer
```

- (Optional) Specify the default service identifier for the service or the service component. This option is useful for the 3GPP Release 8 specifications or for generating a Release 7 service data container.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging charging-profiles profile-name]
user@host# set default-service-id integer
```

- (Optional) Specify the CDR profile referenced by this charging profile. The CDR profile must be defined.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging charging-profiles profile-name]
user@host# set cdr-profile profile-name
```

- (Optional) Specify the trigger profile referenced by this charging profile. The trigger profile must be defined.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging charging-profiles profile-name]
user@host# set trigger-profile profile-name
```

Related Documentation

- [Configuring Charging on page 279](#)
- [Charging Profiles on page 277](#)
- [Configuring S-GW-Specific Charging Parameters on page 280](#)
- [Configuring S-GW Global Charging Profiles and Selection Order on page 282](#)
- [Configuring S-GW Charging Traceoptions on page 284](#)
- [Configuring S-GW Charging Traceoptions on page 284](#)

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:

- 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
```

- 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 Charging on page 279](#)
- [Charging Profiles on page 277](#)
- [Configuring S-GW-Specific Charging Parameters on page 280](#)
- [Configuring S-GW Global Charging Profiles and Selection Order on page 282](#)
- [Configuring S-GW Charging Traceoptions on page 284](#)
- [Configuring S-GW Charging Traceoptions on page 284](#)

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 303](#)
- [Configuring the Tracing Flags on page 303](#)

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. The following table describes the flags that you can include.

Flag	Description
all	Trace all operations
cdr-encoding	Trace CDR encoding
client-fsm	Trace client finite state machine (FSM)
config	Trace configuration events
fsm	Trace FSM
general	Trace general flow

Flag	Description
group-fsm	Trace group FSM
init	Trace initialization events
ipc	Trace IPC
path-management	Trace path management module
request	Trace requests
resource	Trace resources
response	Trace responses
timers	Trace timers
transport	Trace transport group
triggers	Trace trigger information

Related Documentation

- [Configuring Charging on page 279](#)
- [Configuring S-GW-Specific Charging Parameters on page 280](#)
- [Configuring S-GW Global Charging Profiles and Selection Order on page 282](#)
- [Configuring S-GW Charging Traceoptions on page 284](#)
- [Configuring S-GW Charging Traceoptions on page 284](#)

Verifying and Managing the Charging Configuration

Purpose Display or clear information about the charging configuration.

- 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 display information about the trigger profiles:
user@host> **show unified-edge ggsn-pgw charging trigger-profile**
- 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 291](#)
- [Configuring GTP Prime for Charging on page 289](#)
- [Configuring Transport Profiles on page 295](#)
- [Configuring Charging Trigger Events on page 296](#)
- [Configuring S-GW-Specific Charging Parameters on page 280](#)
- [Configuring S-GW Global Charging Profiles and Selection Order on page 282](#)
- [Configuring S-GW Charging Traceoptions on page 284](#)
- [Configuring S-GW Charging Traceoptions on page 284](#)

PART 7

Quality of Service Configuration

- [Configuring Quality of Service on page 309](#)

CHAPTER 12

Configuring Quality of Service

- [Quality of Service Overview on page 310](#)
- [Call Admission Control Overview on page 315](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 317](#)
- [Policing Subscriber Traffic on the Broadband Gateway Overview on page 318](#)
- [Applying Rewrite Rules on Mobile Interfaces Overview on page 319](#)
- [Understanding Upstream and Downstream Processing of ToS Values in GTP-U Packets on page 320](#)
- [Understanding How NQN and Upgrade Flags in PDP Contexts Affect QoS Upgrade Behavior on page 321](#)
- [Configuring QoS on the Broadband Gateway Overview on page 323](#)
- [Configuring the Maximum Number of Bearers on page 324](#)
- [Configuring Bandwidth Pools on page 325](#)
- [Configuring Preemption for Call Admission Control on page 326](#)
- [Configuring Resource Thresholds on a 4G Network on page 326](#)
- [Configuring Resource Thresholds on a 3G Network on page 328](#)
- [Configuring Resource Thresholds for 3G and 4G Networks on page 330](#)
- [Configuring a Classifier Profile for a 4G Network on page 332](#)
- [Configuring a Classifier Profile for a 3G Network on page 333](#)
- [Configuring a Classifier Profile for 3G and 4G Networks on page 334](#)
- [Configuring a CoS Policy Profile for a 4G Network on page 336](#)
- [Configuring a CoS Policy Profile for a 3G Network on page 338](#)
- [Configuring a CoS Policy Profile for 3G and 4G Networks on page 340](#)
- [Configuring a Local Policy on page 343](#)
- [Applying a Local Policy on page 344](#)
- [Configuring Ingress Rewrite Rules for a Mobile Interface on page 345](#)
- [Configuring Egress Rewrite Rules for a Mobile Interface on page 345](#)
- [Applying Ingress Rewrite Rules to a Mobile Interface on page 346](#)
- [Applying Egress Rewrite Rules to Mobile Interfaces on page 347](#)

- [Example: Configuring Quality of Service on page 348](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

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 310](#)
- [Differentiated Services on page 310](#)
- [QoS Parameters in 3G Networks on page 311](#)
- [QoS Parameters in 4G Networks on page 312](#)
- [Aggregate Maximum Bit Rate on page 314](#)
- [Allocation and Retention Priority on page 314](#)
- [Preemption on page 314](#)

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 (4G subscribers).

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 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, each traffic class (and for the Interactive class, traffic class/traffic handling priority) is mapped to a forwarding class and packet loss priority (PLP) in a QoS classifier profile.



NOTE: If traffic is not mapped 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.

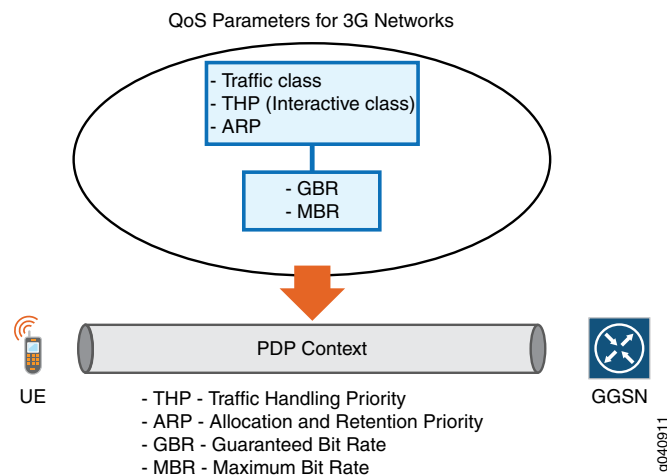
Table 46 on page 311 shows the supported traffic classes, as defined in the 3GPP standards.

Table 46: Traffic Classes for a 3G Network

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 43 on page 312 shows the QoS parameters that the broadband gateway evaluates to determine whether to limit, upgrade, or reject an incoming PDP context request.

Figure 43: Key QoS Parameters for PDP Context Requests



The guaranteed bit rate (GBR), shown in [Figure 43 on page 312](#), 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 43 on page 312](#), 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.

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. QCI values 1 through 4 correspond to dedicated bearers, which the broadband gateway does not support. [Table 47 on page 312](#) shows the supported QoS Class Identifiers and the associated set of QoS characteristics, as defined in the 3GPP standards.

Table 47: QoS Class Identifier for a 4G Network

Qos Class Identifier	Priority	Packet Delay Budget	Packet Error Loss Rate	Example Services
5	1	100 milliseconds (ms)	10^{-6}	IP Multimedia Subsystem(IMS) signaling

Table 47: QoS Class Identifier for a 4G Network (*continued*)

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.

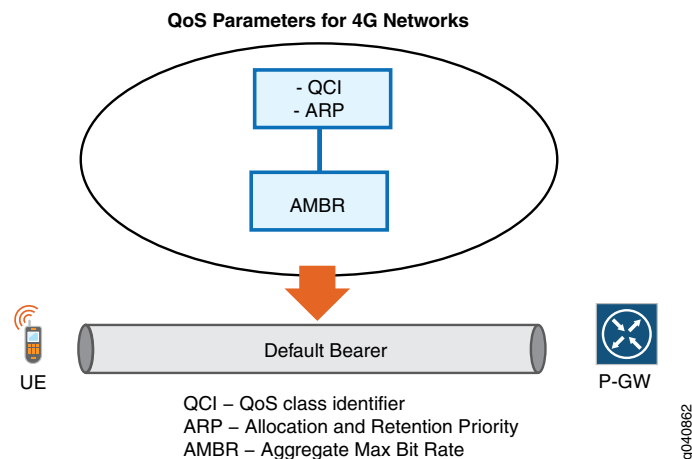
The packet error loss rate defines the percentage of higher layer packets—for example, IP packets—that are lost during periods when the network is not congested.



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 S-Gi 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 44 on page 313 shows the QoS parameters that the broadband gateway processes to determine whether to limit, upgrade, or reject bearer requests.

Figure 44: 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 AMBR defines the maximum allowed throughput for a user equipment 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 over bearers with a lower ARP.

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, ARP values range from 1 through 3, where 1 corresponds to the highest priority and 3 corresponds to the lowest priority. The more sensitive the QoS application, the lower the corresponding PL or ARP value.

Preemption

The broadband gateway uses ARP values to manage the allocation and retention of resources for bearers. When preemption is enabled in a 4G network, the broadband gateway evaluates the PL and the preemption vulnerability (PVI) and preemption capability (PCI) flags in the GTPv2 packet header 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: In a 3G network, PDP context requests do not support the PVI and PCI flags, so when preemption is enabled, the broadband gateway uses ARP values to determine the preemption capability and preemption vulnerability of PDP contexts. You can use the command-line interface (CLI) to independently enable or disable preemption capability and preemption vulnerability.

Related Documentation

- [Call Admission Control Overview on page 315](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 317](#)

- [Applying Rewrite Rules on Mobile Interfaces Overview on page 319](#)
- [Configuring QoS on the Broadband Gateway Overview on page 323](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

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 system, CPU, memory, or bearer load for upstream or downstream traffic exceeds configured CAC thresholds.

This topic covers:

- [Enforcing Call Admission Control on page 315](#)
- [Managing Bandwidth on page 315](#)
- [Managing the Number of Bearers on page 316](#)
- [Managing Resource Thresholds on page 316](#)
- [Default Resource Threshold Settings on page 317](#)

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.
- System load—Specifies a level of traffic flow control when memory utilization, CPU load, and queue depths (for GTP, RADIUS, and CDR) reach a configured lower or upper threshold.



NOTE: System load is an average of memory and CPU load, so the configuration you specify for the system load should take into consideration both memory and CPU load.

- 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, system, 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:

- Low threshold—70 percent for all parameters
- Low threshold ARP—10 (GTPv2) and 2 (GTPv1)
- High threshold—85 percent for all parameters
- High threshold ARP—5 (GTPv2) and 1 (GTPv1)

Related Documentation

- [Quality of Service Overview on page 310](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 317](#)
- [Policing Subscriber Traffic on the Broadband Gateway Overview on page 318](#)
- [Configuring QoS on the Broadband Gateway Overview on page 323](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

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 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 traffic class**—Any bearer set up with a traffic class or traffic handling priority that is of a higher traffic class 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 310](#)
- [Call Admission Control Overview on page 315](#)
- [Configuring QoS on the Broadband Gateway Overview on page 323](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

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, dropping, 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.

In a 4G network, you configure the **violate-action** option to specify the action to take when traffic exceeds the configured aggregate maximum bit rate (AMBR). In a 3G network, you configure the **violate-action** to specify the action to take when traffic exceeds the configured maximum bit rate (MBR), and the **exceed-action** option to specify the action to take when traffic exceeds the configured guaranteed bit rate (GBR).

The broadband gateway supports the following policer actions:

- **exceed-action**—Specifies one of the following actions for packets that exceed the GBR:
 - Set the PLP to “high” (default).
 - Transmit the packet without changing the PLP.
 - Drop the packet.
- **violate-action**—Specifies one of the following actions for packets that exceed the AMBR or MBR:
 - Drop the packet (default).

- Set the PLP to “high”.
- Transmit the packet without changing PLP.

**Related
Documentation**

- [Quality of Service Overview on page 310](#)
- [Call Admission Control Overview on page 315](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 317](#)
- [Configuring QoS on the Broadband Gateway Overview on page 323](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

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 Gn or S5 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 a 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 Gi or SGi 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 310](#)
- [Call Admission Control Overview on page 315](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 317](#)
- [Configuring QoS on the Broadband Gateway Overview on page 323](#)

- [Understanding Upstream and Downstream Processing of ToS Values in GTP-U Packets on page 320](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

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 320](#)
- [Processing of ToS Values for Downstream Subscriber Packets on page 321](#)

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 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 egress 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 egress rewrite rule must be configured and applied to each mobile interface to provide the required DSCP marking for 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 ingress 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-GN 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 319](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

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 45 on page 322](#) shows how negotiated QoS values are affected based on the presence of NQN or Upgrade flags in Create/Update PDP context requests.

Figure 45: 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 45 on page 322](#), 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 45 on page 322](#), 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 45 on page 322](#), 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 317](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

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 (and optionally the percentage of bandwidth to allocate to real-time traffic) for negotiating and reserving bandwidth.

You can specify the **both** keyword to allocate the same bandwidth, unilaterally, for uplink and downlink subscriber traffic, or optionally, configure separate bandwidth pools to allocate bandwidth independently for uplink and downlink subscriber traffic.

3. Configure preemption at the system level to enable preemption for GTPv2 packets. For GTPv1 packets, you can enable preemption capability and preemption vulnerability independently.



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, system load, 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.



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 system 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 315](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 317](#)
- [Policing Subscriber Traffic on the Broadband Gateway Overview on page 318](#)
- [Applying Rewrite Rules on Mobile Interfaces Overview on page 319](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

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 system 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 system 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 323](#)
- [Call Admission Control Overview on page 315](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 317](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)

- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

Configuring Bandwidth Pools

You configure a bandwidth pool 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).

To configure a bandwidth pool:

1. Specify a name for the bandwidth pool.

```
[edit unified-edge cos-cac]
user@host# edit bandwidth-pools bw-pool-1
```

2. Configure the total bandwidth of the pool, in megabits per second (mbps).

```
[edit unified-edge cos-cac bandwidth-pools bw-pool-1]
user@host# set bandwidth 70000
```

3. Allocate bandwidth from the bandwidth pool to the conversational and streaming traffic classes as a percentage of the total bandwidth for the pool:

- a. Allocate a percentage of the total bandwidth to reserve for the conversational traffic class.

```
[edit unified-edge cos-cac bandwidth-pools bw-pool-1]
user@host# set traffic-class conversational percentage 45
```

- b. Allocate the percentage of the total bandwidth to be reserved for the streaming traffic class.

```
[edit unified-edge cos-cac bandwidth-pools bw-pool-1]
user@host# set traffic-class streaming percentage 30
```

4. Specify that when traffic load on the broadband gateway reaches the configured percentage for the streaming traffic class, then Create or Modify PDP context requests can be downgraded.

```
[edit unified-edge cos-cac bandwidth-pools bw-pool-1 traffic-class streaming]
user@host# set downgrade
```

Related Documentation

- [Configuring QoS on the Broadband Gateway Overview on page 323](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

Configuring Preemption for Call Admission Control

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. 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.

To enable preemption on the MobileNext 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 a 3G network:

```
[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 323](#)
- [Call Admission Control Overview on page 315](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 317](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

Configuring Resource Thresholds on a 4G Network

You configure a resource threshold profile to ensure that when the bearer load, system load, CPU load, or memory load at the access point name (APN) or system level on the MobileNext Broadband Gateway reaches a specified threshold, only Create Session requests with a higher PL value are allowed.

To configure a resource threshold profile:

1. Specify a name for the resource threshold profile.

```
[edit unified-edge cos-cac]
user@host# edit resource-threshold-profiles resource-threshold-1
```

2. Configure lower and upper thresholds for the system load and bearer priority level:

- a. Configure a lower limit for the system load. The following configuration specifies that when the system load exceeds 70 percent of the maximum threshold, only Create Session requests with a priority level equal to or higher than 10 are accepted:

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1
 system-load low]
user@host# set percentage 70
user@host# set gtpv2-priority-level 10
```

- b. Configure an upper limit for the system load. The following configuration specifies that when the system load exceeds 85 percent of the maximum threshold, only Create Session requests with a priority level equal to or higher than 4 are accepted:

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1
 system-load low]
user@host# set percentage 85
user@host# set gtpv2-priority-level 4
```

3. Configure lower and upper thresholds for the bearer load and bearer priority level:

- a. Configure a lower threshold for the bearer load. The following configuration specifies that when the number of bearers exceeds 70 percent of the maximum bearers allowed, only Create Session requests with a priority level equal to or higher than 10 are accepted:

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1
 bearers-load low]
user@host# set percentage 70
user@host# set gtpv2-priority-level 10
```

- b. Configure an upper threshold for the bearer load. 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 4 are accepted:

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1
 bearers-load high]
user@host# set percentage 85
user@host# set gtpv2-priority-level 4
```

4. Configure lower and upper thresholds for the CPU load and bearer priority level:

- a. Configure a lower limit for the CPU load. The following configuration specifies that when the CPU load exceeds 70 percent of the maximum threshold, only Create Session requests with a priority level equal to or higher than 10 are accepted:

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1 cpu
 low]
user@host# set percentage 70
user@host# set gtpv2-priority-level 10
```

- b. Configure an upper limit for the CPU load. The following configuration specifies that when the CPU load exceeds 85 percent of the maximum threshold, only Create Session requests with a priority level equal to or higher than 4 are accepted:

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1 cpu
 high]
```

```
user@host# set percentage 85
user@host# set gtpv2-priority-level 4
```

5. Configure lower and upper memory thresholds and bearer priority for the memory load:

- a. Configure a lower limit for the memory load. The following configuration specifies that when the memory usage exceeds 70 percent of the maximum threshold, only Create Session requests with a priority level equal to or higher than 10 are accepted:

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1 memory
low]
user@host# set percentage 70
user@host# set gtpv2-priority-level 10
```

- b. Configure an upper limit for the memory load. The following configuration specifies that when the memory usage exceeds 85 percent of the maximum threshold, only Create Session requests with a priority level equal to or higher than 4 are accepted:

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1 memory
high]
user@host# set percentage 85
user@host# set gtpv2-priority-level 4
```

Related Documentation

- [Configuring QoS on the Broadband Gateway Overview on page 323](#)
- [Call Admission Control Overview on page 315](#)
- [Configuring Resource Thresholds on a 3G Network on page 328](#)
- [Configuring Resource Thresholds for 3G and 4G Networks on page 330](#)
- [Example: Configuring Quality of Service on page 348](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

Configuring Resource Thresholds on a 3G Network

You configure a resource threshold profile to ensure that when the bearer load, system load, CPU load, or memory load at the access point name (APN) or system level on the MobileNext Broadband Gateway reaches a configured threshold, only Create Session requests that meet or exceed the configured allocation and retention priority (ARP) value are accepted.

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 lower and upper thresholds for the system load and ARP priority level:

- a. Configure a lower limit for the system load. The following configuration specifies that when the system load exceeds 70 percent of the maximum threshold, only Create Session requests with a higher priority ARP than 3 are accepted.

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1
system-load low]
user@host# set percentage 70
user@host# set gtpv1-arp 3
```

- b. Configure an upper limit for the system load. The following configuration specifies that when the system load exceeds 85 percent of the maximum threshold, only Create Session requests with a higher priority ARP than 2 are accepted:

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1
system-load low]
user@host# set percentage 85
user@host# set gtpv1-arp 2
```

3. Configure lower and upper thresholds for the bearer load and ARP priority level:

- a. Configure a lower threshold for the bearer load. The following configuration specifies that when the number of bearers exceeds 70 percent of the maximum bearers allowed, only Create Session requests with a higher priority ARP than 3 are accepted:

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1
bearers-load low]
user@host# set percentage 70
user@host# set gtpv1-arp 3
```

- b. Configure an upper threshold for the bearer load. The following configuration specifies that when the number of bearers exceeds 85 percent, only Create Session requests with a higher priority ARP than 2 are accepted:

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1
bearers-load high]
user@host# set percentage 85
user@host# set gtpv1-arp 2
```

4. Configure lower and upper thresholds for the CPU load and ARP level:

- a. Configure a lower limit for the CPU load. The following configuration specifies that when the memory load exceeds 70 percent of the maximum threshold, only Create Session requests with a higher priority ARP than 3 are accepted:

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1 cpu
low]
user@host# set percentage 70
user@host# set gtpv1-arp 3
```

- b. Configure an upper limit for the CPU load. The following configuration specifies that when the CPU load exceeds 85 percent of the maximum threshold, only Create Session requests with a higher priority ARP than 2 are accepted:

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1 cpu
high]
```

```
user@host# set percentage 85
user@host# set gtpv1-arp 2
```

5. Configure lower and upper memory thresholds and the bearer priority for the memory load:

- a. Configure a lower limit for the memory load. The following configuration specifies that when the memory usage exceeds 70 percent of the maximum threshold, only Create Session requests with a higher priority ARP than 3 are accepted:

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1 memory
low]
user@host# set percentage 70
user@host# set gtpv1-arp 3
```

- b. Configure an upper limit for the memory load. The following configuration specifies that when the memory usage exceeds 85 percent of the maximum threshold, only Create Session requests with a higher priority ARP than 2 are accepted:

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1 memory
high]
user@host# set percentage 85
user@host# set gtpv1-arp 2
```

Related Documentation

- [Configuring QoS on the Broadband Gateway Overview on page 323](#)
- [Call Admission Control Overview on page 315](#)
- [Configuring Resource Thresholds on a 4G Network on page 326](#)
- [Configuring Resource Thresholds for 3G and 4G Networks on page 330](#)
- [Example: Configuring Quality of Service on page 348](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

Configuring Resource Thresholds for 3G and 4G Networks

You configure a resource threshold profile to ensure that when the bearer load, system load, CPU load, or memory load at the access point name (APN) or system level on the MobileNext Broadband Gateway reaches a specified threshold, only Create Session requests that meet or exceed a designated allocation and retention priority level are granted.

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 60 percent of the allowed limit, only Create Session requests with a priority level equal to or higher the specified ARP values are accepted:

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1
  bearers-load low]
user@host# set percentage 70
user@host# set gtpv1-arp 3
user@host# set gtpv2-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 80 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 gtpv1-arp 2
user@host# set gtpv2-priority-level 4
```

3. Configure the bearer priority and threshold limits for the system load:

- a. Configure a lower limit for the system load.

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1
  system-load low]
user@host# set percentage 70
user@host# set gtpv1-arp 3
user@host# set gtpv2-priority-level 10
```

- b. Configure an upper limit for the system load.

```
[edit unified-edge cos-cac resource-threshold-profiles resource-threshold-1
  system-load high]
user@host# set percentage 85
user@host# set gtpv1-arp 2
user@host# set gtpv2-priority-level 4
```

4. 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 gtpv1-arp 3
user@host# set gtpv2-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 gtpv1-arp 2
```

```
user@host# set gtpv2-priority-level 4
```

5. 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 gtpv1-arp 3
user@host# set gtpv2-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 gtpv1-arp 3
user@host# set gtpv2-priority-level 10
```

Related Documentation

- [Configuring QoS on the Broadband Gateway Overview on page 323](#)
- [Call Admission Control Overview on page 315](#)
- [Configuring Resource Thresholds on a 4G Network on page 326](#)
- [Configuring Resource Thresholds on a 3G Network on page 328](#)
- [Example: Configuring Quality of Service on page 348](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

Configuring a Classifier Profile for a 4G Network

A classifier profile defines the QoS Class Identifiers (QCIs) for a Packet Data Network Gateway (P-GW). You configure QCI values to define the packet-forwarding treatment for each bearer. A QCI is associated with priority, delay, and packet loss values. The MobileNext Broadband Gateway supports only QCI values for default bearers, which do not require dedicated resource allocation for a guaranteed bit rate (GBR).

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 the QCI values and the associated QoS characteristics based on traffic requirements:

- a. Configure a QCI value and the associated forwarding class and loss priority for IP Multimedia Subsystem (IMS) signaling traffic.

```
[edit unified-edge cos-cac classifier-profiles classifier-profile-1]
```

```

user@host# set qos-class-identifier 5
user@host# set forwarding-class af2
user@host# set loss-priority low

```

- b. Configure a QCI value and the associated forwarding class and loss priority for video (buffered streaming) traffic.

```

[edit unified-edge cos-cac classifier-profiles classifier-profile-1]
user@host# set qos-class-identifier 6
user@host# set forwarding-class af2
user@host# set loss-priority low

```

- c. Configure a QCI value and the associated forwarding class and loss priority for voice, video (live streaming), and interactive gaming traffic.

```

[edit unified-edge cos-cac classifier-profiles classifier-profile-1]
user@host# set qos-class-identifier 7
user@host# set forwarding-class af3
user@host# set loss-priority low

```

- d. Configure a QCI value and the associated forwarding class and loss priority for background traffic.

```

[edit unified-edge cos-cac classifier-profiles classifier-profile-1]
user@host# set qos-class-identifier 8
user@host# set forwarding-class be
user@host# set loss-priority low

```

Related Documentation

- [Configuring QoS on the Broadband Gateway Overview on page 323](#)
- [Configuring a Classifier Profile for a 3G Network on page 333](#)
- [Configuring a Classifier Profile for 3G and 4G Networks on page 334](#)
- [Example: Configuring Quality of Service on page 348](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

Configuring a Classifier Profile for a 3G Network

A classifier profile defines the traffic classes for a gateway GPRS support node (GGSN). You configure the traffic classes to define the packet-forwarding treatment by assigning a forwarding class and packet loss priority. You can configure conversational, streaming, interactive, and background traffic classes to manage traffic based on delay, jitter, bandwidth, and reliability.

To configure a classifier profile to define the traffic classes for the MobileNext Broadband Gateway:

1. Specify a name for the classifier profile.

```

[edit unified-edge cos-cac]
user@host# edit classifier-profiles classifier-profile-1

```

2. Configure each traffic class in the classifier profile based on the degree to which typical services representing a specific traffic class are delay sensitive.

- a. Configure the conversational traffic class.

```
[edit unified-edge cos-cac classifier-profiles classifier_profile_1]
user@host# set traffic-class conversational
user@host# set forwarding-class ef
user@host# set loss-priority low
```

- b. Configure the streaming traffic class.

```
[edit unified-edge cos-cac classifier-profiles classifier_profile_1]
user@host# set traffic-class streaming
user@host# set forwarding-class af2
user@host# set loss-priority low
```

- c. Configure the interactive traffic class.

```
[edit unified-edge cos-cac classifier-profiles classifier_profile_1]
user@host# set traffic-class interactive
user@host# set traffic-handling-priority 2
user@host# set forwarding-class af3
user@host# set loss-priority low
```

- d. Configure the background traffic class:

```
[edit unified-edge cos-cac classifier-profiles classifier_profile_1]
user@host# set traffic-class background
user@host# set forwarding-class be
user@host# set loss-priority high
```

Related Documentation

- [Configuring QoS on the Broadband Gateway Overview on page 323](#)
- [Configuring a Classifier Profile for a 4G Network on page 332](#)
- [Configuring a Classifier Profile for 3G and 4G Networks on page 334](#)
- [Example: Configuring Quality of Service on page 348](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

Configuring a Classifier Profile for 3G and 4G Networks

A classifier profile defines the QoS classification for a MobileNext Broadband Gateway configured as a gateway GPRS support node/Packet Data Network Gateway (GGSN/P-GW). You configure the traffic classes and QoS Class Identifier (QCI) values to define the packet-forwarding treatment for bearers. Each traffic class and QCI is associated with priority, delay, and packet loss values.

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 each traffic class in the classifier profile based on the degree to which typical services representing a specific traffic class are delay sensitive:

- a. Configure the conversational traffic class.

```
[edit unified-edge cos-cac classifier-profiles classifier-profile-1]
user@host# set traffic-class conversational
user@host# set forwarding-class ef
user@host# set loss-priority low
```

- b. Configure the streaming traffic class.

```
[edit unified-edge cos-cac classifier-profiles classifier-profile-1]
user@host# set traffic-class streaming
user@host# set forwarding-class af2
user@host# set loss-priority low
```

- c. Configure the interactive traffic class.

```
[edit unified-edge cos-cac classifier-profiles classifier-profile-1]
user@host# set traffic-class interactive
user@host# set traffic-handling-priority 2
user@host# set forwarding-class af3
user@host# set loss-priority low
```

- d. Configure the background traffic class.

```
[edit unified-edge cos-cac classifier-profiles classifier-profile-1]
user@host# set traffic-class background
user@host# set forwarding-class be
user@host# set loss-priority high
```

3. Configure the QCI values and the associated QoS characteristics based on traffic requirements:

- a. Configure a QCI value and the associated forwarding class and loss priority for IP Multimedia Subsystem (IMS) signaling traffic.

```
[edit unified-edge cos-cac classifier-profiles classifier-profile-1]
user@host# set qos-class-identifier 5
user@host# set forwarding-class af2
user@host# set loss-priority low
```

- b. Configure a QCI value and the associated forwarding class and loss priority for video (buffered streaming) traffic.

```
[edit unified-edge cos-cac classifier-profiles classifier-profile-1]
user@host# set qos-class-identifier 6
user@host# set forwarding-class af2
user@host# set loss-priority low
```

- c. Configure a QCI value and the associated forwarding class and loss priority for voice, video (live streaming), and interactive gaming traffic.

```
[edit unified-edge cos-cac classifier-profiles classifier-profile-1]
user@host# set qos-class-identifier 7
```

```
user@host# set forwarding-class af3
user@host# set loss-priority low
```

- d. Configure a QCI value and the associated forwarding class and loss priority for background traffic.

```
[edit unified-edge cos-cac classifier-profiles classifier-profile-1]
user@host# set qos-class-identifier 8
user@host# set forwarding-class be
user@host# set loss-priority low
```

Related Documentation

- [Configuring QoS on the Broadband Gateway Overview on page 323](#)
- [Configuring a Classifier Profile for a 4G Network on page 332](#)
- [Configuring a Classifier Profile for a 3G Network on page 333](#)
- [Example: Configuring Quality of Service on page 348](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

Configuring a CoS Policy Profile for a 4G Network

In a 4G network, a class-of-service (CoS) policy profile defines the highest quality-of-service (QoS) Class Identifier (QCI) value that can be accepted at the access point name (APN) level or system level, the aggregate maximum bit rate (AMBR) for default bearers, and the allocation and retention priority (ARP). A CoS policy profile also specifies the policer action to take when subscriber traffic exceeds the configured AMBR.

By default, when a bearer request has a higher AMBR value than the value configured in the CoS policy profile, the bearer request is downgraded.

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-1
```

2. Specify the highest QCI that can be accepted at the APN or system level, and specify **upgrade** to allow bearers with a lower priority QCI value to be upgraded to a higher priority QCI value.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-1]
user@host# set qos-class-identifier 5 upgrade
```

3. Configure the aggregate maximum bit rate for traffic:
 - a. Configure the aggregate maximum bit rate for downlink traffic.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-1
 aggregated-maximum-bit-rate]
user@host# set downlink 250000
```

- b. Configure the aggregate maximum bit rate for uplink traffic.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-1
 aggregated-maximum-bit-rate]
user@host# set uplink 70000
```



NOTE: When you configure the AMBR, you can either specify both or uplink and downlink, but you cannot configure both with either the uplink or downlink option. In addition, if you specify the uplink option, you must also specify the downlink option.

- c. Configure the policy profile to either upgrade or reject bearer requests based on the AMBR value specified in the user packet:

- To upgrade bearer requests that specify a lower AMBR than the configured AMBR:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-1
 aggregated-maximum-bit-rate]
user@host# set upgrade
```

- To reject new bearer requests that specify a higher AMBR than the configured AMBR.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-1
 aggregated-maximum-bit-rate]
user@host# set reject
```



NOTE: When the reject option is configured, the broadband gateway rejects any Create Session requests with a higher AMBR value than the configured AMBR. However, Modify bearer requests with a higher AMBR value are downgraded to the configured AMBR.

4. Specify that bearer requests with a lower allocation and retention priority level (PL) than the configured value can be upgraded.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-1
 allocation-retention-priority]
user@host# set gtpv2-priority-value 7 upgrade
```

5. Configure the action to take when the AMBR of bearer traffic exceeds the peak rate.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-1
 aggregated-maximum-bit-rate]
user@host# set violate-action set-loss-priority-high
```



NOTE: By default, traffic that exceeds the peak AMBR is dropped.

Related Documentation

- [Class of Service \(CoS\) Policy Profile Overview on page 317](#)
- [Configuring QoS on the Broadband Gateway Overview on page 323](#)
- [Configuring a CoS Policy Profile for a 3G Network on page 338](#)
- [Configuring a CoS Policy Profile for 3G and 4G Networks on page 340](#)
- [Example: Configuring Quality of Service on page 348](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

Configuring a CoS Policy Profile for a 3G Network

In a 3G network, a class-of-service (CoS) policy profile defines the highest traffic class (and highest priority for the interactive traffic class) that can be accepted at an access point name (APN), and for each traffic class, the maximum bit rate (MBR) and the guaranteed bit rate (GBR). A CoS policy profile also specifies the policer action to take when subscriber traffic exceeds the configured GBR, MBR, or both.

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. Specify the highest traffic class and, for the interactive class only, the highest traffic handling priority for a PDP context request. Also, allow PDP contexts with a lower-priority traffic class to be upgraded to a higher-priority traffic class.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2]
user@host# set traffic-class interactive priority2 upgrade
```

3. Specify that the broadband gateway accepts only PDP contexts with a higher allocation and retention priority (ARP) value than the configured ARP when thresholds are exceeded at the APN or system level, and allow the ARP value of a PDP context request to be upgraded.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2
allocation-retention-priority]
user@host# set gtpv1-arp 3
```

4. Configure an MBR for each traffic class. Optionally, you can configure different MBRs for uplink and downlink traffic.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 maximum-bit-rate
traffic-class]
```



```

user@host# set streaming uplink 50000
user@host# set streaming downlink 200000
user@host# set interactive uplink 200000
user@host# set interactive downlink 200000
user@host# set conversational both 250000
user@host# set background both 20000

```

5. Upgrade PDP context requests that have a lower MBR than the configured MBR for a traffic class.

```

[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 maximum-bit-rate
traffic-class]
user@host# set upgrade

```

6. Configure a GBR for traffic classes. Optionally, you can configure different GBRs for uplink and downlink traffic.

```

[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 guaranteed-bit-rate
traffic-class]
user@host# set streaming uplink 50000
user@host# set streaming downlink 200000
user@host# set conversational uplink 100000
user@host# set conversational downlink 200000

```



NOTE: When you configure the MBR or GBR for a given traffic class, you can either specify both or uplink and downlink, but you cannot configure a traffic class using both with either the uplink or downlink option. In addition, if you specify the uplink option, you must also specify the downlink option for the traffic class.

7. Configure the action to take when the MBR for a traffic class exceeds the configured value.

```

[edit unified-edge cos-cac cos-policy-profiles policy-profile-2]
user@host# set violate-action set-loss-priority-high

```



NOTE: By default, traffic that exceeds the peak rate is dropped.

8. Configure the action to take when the actual bit rate for a traffic class exceeds the configured GBR.

```

[edit unified-edge cos-cac cos-policy-profiles policy-profile-2]
user@host# set exceed-action drop

```



NOTE: By default, when subscriber traffic exceeds the peak rate, the PLP is set to “High” and the packet is transmitted.

Related Documentation

- [Class of Service \(CoS\) Policy Profile Overview on page 317](#)
- [Configuring QoS on the Broadband Gateway Overview on page 323](#)

- [Configuring a CoS Policy Profile for a 4G Network on page 336](#)
- [Configuring a CoS Policy Profile for 3G and 4G Networks on page 340](#)
- [Example: Configuring Quality of Service on page 348](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

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 that can be accepted at an access point name (APN) or system level, the MBR and GBR for bearers, and the allocation and retention priority (ARP). 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.

In a 4G network, a CoS policy profile defines the highest QoS Class Identifier (QCI) value that can be accepted at the APN level or system level, the aggregate maximum bit rate (AMBR) for default bearers, and the allocation and retention priority. A CoS policy also specifies the policer action when subscriber traffic exceeds the configured AMBR. By default, when a bearer request has a higher AMBR value than the value configured in the CoS policy profile, the 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. Configure the highest QCI that can be accepted at the APN or system level, and specify **upgrade** to allow bearers with a lower QCI value to be upgraded to a higher QCI value.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2]  
user@host# set qos-class-identifier 5 upgrade
```

3. Configure the highest traffic class and, for the interactive traffic class, the maximum traffic handling priority that can be accepted for a PDP context.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2]  
user@host# set traffic-class interactive priority 2
```

4. Configure the aggregate maximum bit rate for traffic:
 - a. Configure the aggregate maximum bit rate for downlink traffic.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2
 aggregated-maximum-bit-rate]
user@host# set downlink 250000
```

- b. Configure the aggregate maximum bit rate for uplink traffic.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2
 aggregated-maximum-bit-rate]
user@host# set uplink 100000
```



NOTE: When you configure the aggregate maximum bit rate, you can either specify both or uplink and downlink, but you cannot configure both with either the uplink or downlink option. In addition, if you specify the uplink option, you must also specify the downlink option for the traffic class.

- c. Configure the policy profile to either upgrade or reject bearer requests based on the AMBR value specified in the user packet:

- To upgrade bearer requests that specify a lower AMBR than the configured AMBR:

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2
 aggregated-maximum-bit-rate]
user@host# set upgrade
```

- To reject new bearer requests that specify a higher AMBR than the configured AMBR.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2
 aggregated-maximum-bit-rate]
user@host# set reject
```



NOTE: When the reject option is configured, the broadband gateway rejects any Create Session requests with higher AMBR value than the configured AMBR. However, Modify bearer requests with a higher AMBR value are downgraded to the configured AMBR.

5. Specify that only bearer requests with a higher allocation and retention priority (PL) value than the configured value are accepted when thresholds are exceeded at the APN level or system level, and allow the PL value of a lower-priority bearer request to be upgraded.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2
 allocation-retention-priority]
user@host# set gtpv2-priority-value 7 upgrade
```

6. Specify that only PDP context requests with a higher-priority ARP value than the configured ARP value are accepted when thresholds are exceeded at the APN level or system level, and allow the ARP value of a lower-priority bearer request to be upgraded.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2
 allocation-retention-priority]
user@host# set gtpv1-priority-value 3 upgrade
```

7. Configure an MBR for each traffic class.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 maximum-bit-rate
 traffic-class]
user@host# set streaming uplink 50000
user@host# set streaming downlink 200000
user@host# set interactive uplink 200000
user@host# set interactive downlink 200000
user@host# set conversational both 250000
user@host# set background both 20000
```



NOTE: When you configure the MBR or GBR for a given traffic class, you can either specify both or uplink and downlink, but you cannot configure a traffic class using both with either the uplink or downlink option. In addition, if you specify the uplink option, you must also specify the downlink option for the traffic class.

8. Allow PDP context requests that have a lower MBR than the configured MBR to be upgraded.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 maximum-bit-rate
 traffic-class]
user@host# set upgrade
```

9. Configure a GBR (in kbps) for streaming and conversational traffic classes. Optionally, you can configure different GBRs for uplink and downlink traffic.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2 guaranteed-bit-rate
 traffic-class]
user@host# set streaming uplink 50000
user@host# set streaming downlink 200000
user@host# set conversational uplink 100000
user@host# set conversational downlink 200000
```

10. Configure the action to take when the MBR for a traffic class, or the AMBR for default bearers, exceeds the configured value.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2]
user@host# set violate-action set-loss-priority-high
```



NOTE: By default, traffic that exceeds the peak rate is dropped.

11. Configure the action to take when the GBR for a traffic class of subscriber traffic exceeds the configured GBR.

```
[edit unified-edge cos-cac cos-policy-profiles policy-profile-2]
user@host# set exceed-action transmit
```



NOTE: By default, traffic that exceeds the peak rate is set to PLP HIGH and transmit.

Related Documentation

- [Class of Service \(CoS\) Policy Profile Overview on page 317](#)
- [Configuring QoS on the Broadband Gateway Overview on page 323](#)
- [Configuring a CoS Policy Profile for a 4G Network on page 336](#)
- [Configuring a CoS Policy Profile for a 3G Network on page 338](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

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 323](#)
- [Configuring the Maximum Number of Bearers on page 324](#)
- [Configuring Bandwidth Pools on page 325](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

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 343](#)
- [Configuring the Maximum Number of Bearers on page 324](#)

- [Configuring Bandwidth Pools on page 325](#)
- [Configuring QoS on the Broadband Gateway Overview on page 323](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

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 319](#)
- [Configuring Egress Rewrite Rules for a Mobile Interface on page 345](#)
- [Configuring QoS on the Broadband Gateway Overview on page 323](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

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 319](#)
- [Configuring QoS on the Broadband Gateway Overview on page 323](#)
- [Configuring Ingress Rewrite Rules for a Mobile Interface on page 345](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

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 319](#)
- [Configuring QoS on the Broadband Gateway Overview on page 323](#)
- [Applying Egress Rewrite Rules to Mobile Interfaces on page 347](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

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 319](#)
- [Configuring QoS on the Broadband Gateway Overview on page 323](#)
- [Applying Ingress Rewrite Rules to a Mobile Interface on page 346](#)

Example: Configuring Quality of Service

This example describes how to configure quality of service (QoS) on the MobileNext Broadband Gateway, and consists of the following sections:

- [Requirements on page 348](#)
- [Overview on page 348](#)
- [Configuration on page 349](#)
- [Verification on page 381](#)

Requirements

This example uses the following hardware and software components:

- An operational MX Series chassis
- Junos OS Mobility 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, email, and file sharing), each of which have different QoS requirements in terms of required bit rates, acceptable packet loss rates, and packet delay. To define the QoS treatment for 3G and 4G subscriber traffic on the broadband gateway, you configure the following QoS components:

- Classifier profiles—Define the mapping of each traffic class and QoS Class Identifier to a forwarding class and packet loss priority. You configure a separate classifier profiles for home, visiting, and roaming subscribers in 3G and 4G networks.
- Resource threshold profiles—Define the thresholds for number of bearers, system load, 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 separate resource threshold profiles for 3G, 4G, and system-level (3G/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 a 3G Network on page 350](#)
- [Configuring Classifier Profiles for Home Subscribers on a 4G Network on page 351](#)
- [Configuring Classifier Profiles for Roaming Subscribers on a 3G Network on page 351](#)
- [Configuring Classifier Profiles for Roaming Subscribers on a 4G Network on page 352](#)
- [Configuring Classifier Profiles for Visitor Subscribers on a 3G Network on page 353](#)
- [Configuring Classifier Profiles for Visitor Subscribers on a 4G Network on page 353](#)
- [Configuring a System-Wide Classifier Profile on page 354](#)
- [Configuring a Resource Threshold Profile for Subscribers on a 3G Network on page 355](#)
- [Configuring a Resource Threshold Profile for Subscribers on a 4G Network on page 357](#)
- [Configuring a System-Wide Resource Threshold Profile on page 359](#)
- [Configuring a CoS Policy Profile for Home Subscribers on a 3G Network on page 361](#)
- [Configuring a CoS Policy Profile for Home Subscribers on a 4G Network on page 363](#)
- [Configuring a CoS Policy Profile for Roaming Subscribers on a 3G Network on page 364](#)
- [Configuring a CoS Policy Profile for Roaming Subscribers on a 4G Network on page 365](#)
- [Configuring a CoS Policy Profile for Visiting Subscribers in a 3G Network on page 366](#)
- [Configuring a CoS Policy Profile for Visiting Subscribers in a 4G Network on page 367](#)
- [Configuring a System-Wide CoS Policy Profile on page 368](#)
- [Configuring Bandwidth Pools on page 370](#)
- [Configuring a Local Policy for 3G Networks on page 370](#)
- [Configuring a Local Policy for 4G Networks on page 372](#)
- [Configuring a System-Wide Local Policy on page 373](#)

- [Applying the Local Policies on page 374](#)
- [Configuring DSCP Ingress Rewrite Rules for IPv4 Packets on page 375](#)
- [Configuring DSCP Ingress Rewrite Rules for IPv6 Packets on page 375](#)
- [Configuring DSCP Egress Rewrite Rules for IPv4 Packets on page 376](#)
- [Configuring DSCP Egress Rewrite Rules for IPv6 Packets on page 377](#)
- [Applying Ingress Rewrite Rules to Mobile Interfaces for 3G and 4G Subscriber Traffic on page 378](#)
- [Applying Egress Rewrite Rules to Mobile Interfaces for 3G and 4G Subscriber Traffic on page 379](#)
- [Configuring the Maximum Number of Bearers on page 380](#)
- [Enabling Preemption on page 380](#)

Configuring Classifier Profiles 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 classifier-profiles home_v1 traffic-class conversational
  forwarding-class af1 loss-priority low
set unified-edge cos-cac classifier-profiles home_v1 traffic-class streaming forwarding-class
  af2 loss-priority low
set unified-edge cos-cac classifier-profiles home_v1 traffic-class background
  forwarding-class ef loss-priority high
set unified-edge cos-cac classifier-profiles home_v1 traffic-class interactive
  traffic-handling-priority 1 forwarding-class af3 loss-priority low
set unified-edge cos-cac classifier-profiles home_v1 traffic-class interactive
  traffic-handling-priority 2 forwarding-class af4 loss-priority low
set unified-edge cos-cac classifier-profiles home_v1 traffic-class interactive
  traffic-handling-priority 3 forwarding-class af5 loss-priority low
```

Step-by-Step Procedure

To configure a classifier profile for home subscribers on a 3G network:

1. Specify a name for the home classifier profile and map each traffic class to a forwarding class and packet loss priority.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_v1 traffic-class
  conversational forwarding-class af1 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_v1 traffic-class
  streaming forwarding-class af2 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_v1 traffic-class
  background forwarding-class ef loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_v1 traffic-class
  interactive traffic-handling-priority 1 forwarding-class af3 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_v1 traffic-class
  interactive traffic-handling-priority 2 forwarding-class af4 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_v1 traffic-class
  interactive traffic-handling-priority 3 forwarding-class af5 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 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 classifier-profiles home_v2 qos-class-identifier 5 forwarding-class af1 loss-priority low
set unified-edge cos-cac classifier-profiles home_v2 qos-class-identifier 6 forwarding-class af2 loss-priority low
set unified-edge cos-cac classifier-profiles home_v2 qos-class-identifier 7 forwarding-class af3 loss-priority low
set unified-edge cos-cac classifier-profiles home_v2 qos-class-identifier 8 forwarding-class af4 loss-priority low
set unified-edge cos-cac classifier-profiles home_v2 qos-class-identifier 9 forwarding-class af5 loss-priority low
```

Step-by-Step Procedure To configure a classifier profile for home subscribers on a 4G network:

- Specify a name for the home classifier profile and map each QoS Class Identifier to a forwarding class and packet loss priority.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_v2 qos-class-identifier 5 forwarding-class af1 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_v2 qos-class-identifier 6 forwarding-class af2 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_v2 qos-class-identifier 7 forwarding-class af3 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_v2 qos-class-identifier 8 forwarding-class af4 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles home_v2 qos-class-identifier 9 forwarding-class af5 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 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 classifier-profiles roamer_v1 traffic-class conversational
  forwarding-class af1 loss-priority high
set unified-edge cos-cac classifier-profiles roamer_v1 traffic-class streaming
  forwarding-class af2 loss-priority high
set unified-edge cos-cac classifier-profiles roamer_v1 traffic-class background
  forwarding-class be loss-priority low
set unified-edge cos-cac classifier-profiles roamer_v1 traffic-class interactive
  traffic-handling-priority 1 forwarding-class af3 loss-priority high
set unified-edge cos-cac classifier-profiles roamer_v1 traffic-class interactive
  traffic-handling-priority 2 forwarding-class af4 loss-priority high
set unified-edge cos-cac classifier-profiles roamer_v1 traffic-class interactive
  traffic-handling-priority 3 forwarding-class af5 loss-priority high

```

Step-by-Step Procedure

To configure classifier profiles for roaming subscribers on a 3G network:

- Specify a name for the roamer classifier profile and map each traffic class to a forwarding class and packet loss priority.

```

[edit]
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_v1 traffic-class
  conversational forwarding-class af1 loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_v1 traffic-class
  streaming forwarding-class af2 loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_v1 traffic-class
  background forwarding-class be loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_v1 traffic-class
  interactive traffic-handling-priority 1 forwarding-class af3 loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_v1 traffic-class
  interactive traffic-handling-priority 2 forwarding-class af4 loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_v1 traffic-class
  interactive traffic-handling-priority 3 forwarding-class af5 loss-priority high

```

Configuring Classifier Profiles 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 classifier-profiles roamer_v2 qos-class-identifier 5 forwarding-class
  af3 loss-priority low
set unified-edge cos-cac classifier-profiles roamer_v2 qos-class-identifier 6
  forwarding-class af4 loss-priority low
set unified-edge cos-cac classifier-profiles roamer_v2 qos-class-identifier 7 forwarding-class
  af5 loss-priority low
set unified-edge cos-cac classifier-profiles roamer_v2 qos-class-identifier 8
  forwarding-class ef loss-priority high
set unified-edge cos-cac classifier-profiles roamer_v2 qos-class-identifier 9
  forwarding-class be loss-priority high

```

Step-by-Step Procedure

To configure classifier profiles for roaming subscribers on a 4G network:

- For a 4G network, specify a name for the roamer classifier profile and map each QoS Class Identifier to a forwarding class and packet loss priority.

```
[edit]
```

```

user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_v2
qos-class-identifier 5 forwarding-class af3 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_v2
qos-class-identifier 6 forwarding-class af4 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_v2
qos-class-identifier 7 forwarding-class af5 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_v2
qos-class-identifier 8 forwarding-class ef loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles roamer_v2
qos-class-identifier 9 forwarding-class be loss-priority high

```

Configuring Classifier Profiles for Visitor 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 classifier-profiles visitor_v1 traffic-class conversational
forwarding-class af2 loss-priority high
set unified-edge cos-cac classifier-profiles visitor_v1 traffic-class streaming forwarding-class
af3 loss-priority high
set unified-edge cos-cac classifier-profiles visitor_v1 traffic-class background
forwarding-class nc loss-priority high
set unified-edge cos-cac classifier-profiles visitor_v1 traffic-class interactive
traffic-handling-priority 1 forwarding-class af4 loss-priority high
set unified-edge cos-cac classifier-profiles visitor_v1 traffic-class interactive
traffic-handling-priority 2 forwarding-class af5 loss-priority low
set unified-edge cos-cac classifier-profiles visitor_v1 traffic-class interactive
traffic-handling-priority 3 forwarding-class be loss-priority high

```

Step-by-Step Procedure To configure classifier profiles for visitor subscribers on a 3G network:

1. Specify a name for the visitor classifier profile and map each traffic class to a forwarding class and packet loss priority.

```

user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_v1 traffic-class
conversational forwarding-class af2 loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_v1 traffic-class
streaming forwarding-class af3 loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_v1 traffic-class
background forwarding-class nc loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_v1 traffic-class
interactive traffic-handling-priority 1 forwarding-class af4 loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_v1 traffic-class
interactive traffic-handling-priority 2 forwarding-class af5 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_v1 traffic-class
interactive traffic-handling-priority 3 forwarding-class be loss-priority high

```

Configuring Classifier Profiles for Visitor 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 classifier-profiles visitor_v2 qos-class-identifier 5 forwarding-class
  af4 loss-priority high
set unified-edge cos-cac classifier-profiles visitor_v2 qos-class-identifier 6 forwarding-class
  af5 loss-priority high
set unified-edge cos-cac classifier-profiles visitor_v2 qos-class-identifier 7 forwarding-class
  ef loss-priority high
set unified-edge cos-cac classifier-profiles visitor_v2 qos-class-identifier 8 forwarding-class
  be loss-priority high
set unified-edge cos-cac classifier-profiles visitor_v2 qos-class-identifier 9 forwarding-class
  nc loss-priority high
```

**Step-by-Step
Procedure**

To configure classifier profiles for visitor subscribers on a 4G network:

1. Specify a name for the visitor classifier profile and map each QoS Class Identifier to a forwarding class and packet loss priority.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_v2
  qos-class-identifier 5 forwarding-class af4 loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_v2
  qos-class-identifier 6 forwarding-class af5 loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_v2
  qos-class-identifier 7 forwarding-class ef loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_v2
  qos-class-identifier 8 forwarding-class be loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles visitor_v2
  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 traffic-class conversational
  forwarding-class af2 loss-priority low
set unified-edge cos-cac classifier-profiles system_wide traffic-class streaming
  forwarding-class af3 loss-priority low
set unified-edge cos-cac classifier-profiles system_wide traffic-class background
  forwarding-class be loss-priority high
set unified-edge cos-cac classifier-profiles system_wide traffic-class interactive
  traffic-handling-priority 1 forwarding-class a4 loss-priority high
set unified-edge cos-cac classifier-profiles system_wide traffic-class interactive
  traffic-handling-priority 2 forwarding-class nc loss-priority high
set unified-edge cos-cac classifier-profiles system_wide traffic-class interactive
  traffic-handling-priority 3 forwarding-class ef loss-priority high
set unified-edge cos-cac classifier-profiles system_wide qos-class-identifier 5
  forwarding-class af2 loss-priority low
set unified-edge cos-cac classifier-profiles system_wide qos-class-identifier 6
  forwarding-class af3 loss-priority low
set unified-edge cos-cac classifier-profiles system_wide qos-class-identifier 7
  forwarding-class af4 loss-priority low
set unified-edge cos-cac classifier-profiles system_wide qos-class-identifier 8
  forwarding-class af5 loss-priority high
```



```
set unified-edge cos-cac classifier-profiles system_wide qos-class-identifier 9
forwarding-class ef 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 traffic class to a forwarding class and packet loss priority.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles system_wide
traffic-class conversational forwarding-class af2 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles system_wide
traffic-class streaming forwarding-class af3 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles system_wide
traffic-class background forwarding-class be loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles system_wide
traffic-class interactive traffic-handling-priority 1 forwarding-class a4 loss-priority
high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles system_wide
traffic-class interactive traffic-handling-priority 2 forwarding-class nc loss-priority
high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles system_wide
traffic-class interactive traffic-handling-priority 3 forwarding-class ef loss-priority
high
```

2. In the **system_wide** classifier profile, map each QoS Classifier 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 5 forwarding-class af2 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles system_wide
qos-class-identifier 6 forwarding-class af3 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles system_wide
qos-class-identifier 7 forwarding-class af4 loss-priority low
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles system_wide
qos-class-identifier 8 forwarding-class af5 loss-priority high
user@ggsn-pgw# set unified-edge cos-cac classifier-profiles system_wide
qos-class-identifier 9 forwarding-class ef 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 Resource Threshold Profile for 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 resource-threshold-profiles resource_v1 bearers-load low
percentage 60
```

```

set unified-edge cos-cac resource-threshold-profiles resource_v1 bearers-load low gtpv1-arp
2
set unified-edge cos-cac resource-threshold-profiles resource_v1 bearers-load high
percentage 80
set unified-edge cos-cac resource-threshold-profiles resource_v1 bearers-load high gtpv1-arp
1
set unified-edge cos-cac resource-threshold-profiles resource_v1 cpu low percentage 70
set unified-edge cos-cac resource-threshold-profiles resource_v1 cpu low gtpv1-arp 2
set unified-edge cos-cac resource-threshold-profiles resource_v1 cpu high percentage 80
set unified-edge cos-cac resource-threshold-profiles resource_v1 cpu high gtpv1-arp 1
set unified-edge cos-cac resource-threshold-profiles resource_v1 system-load low
percentage 85
set unified-edge cos-cac resource-threshold-profiles resource_v1 system-load low gtpv1-arp
2
set unified-edge cos-cac resource-threshold-profiles resource_v1 system-load high
percentage 90
set unified-edge cos-cac resource-threshold-profiles resource_v1 system-load high gtpv1-arp
1
set unified-edge cos-cac resource-threshold-profiles resource_v1 memory low percentage
85
set unified-edge cos-cac resource-threshold-profiles resource_v1 memory low gtpv1-arp
2
set unified-edge cos-cac resource-threshold-profiles resource_v1 memory high percentage
90
set unified-edge cos-cac resource-threshold-profiles resource_v1 memory high gtpv1-arp
1

```

Step-by-Step Procedure

To configure resource threshold profiles for subscribers on a 3G network:

1. Specify a name for the resource threshold profile and configure the low and high thresholds for bearer load, CPU load, system load, and memory load.


```

[edit]
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v1
bearers-load low percentage 60
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v1
bearers-load low gtpv1-arp 2
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v1
bearers-load high percentage 80
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v1
bearers-load high gtpv1-arp 1

```
2. Configure the low and high thresholds for the CPU load.


```

[edit]
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v1
cpu low percentage 70
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v1
cpu low gtpv1-arp 2
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v1
cpu high percentage 80
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v1
cpu high gtpv1-arp 4

```
3. Configure the low and high thresholds for the system load.


```

[edit]

```

```

user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v1
system-load low percentage 85
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v1
system-load low gtpv1-arp 2
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v1
system-load high percentage 90
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v1
system-load high gtpv1-arp 1

```



NOTE: System load is an average of memory and CPU, so the values you specify for the system load should take into consideration values specified for the memory and CPU load.

4. Configure the low and high thresholds for the memory load.

```

[edit]
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v1
memory low percentage 85
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v1
memory low gtpv1-arp 2
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v1
memory high percentage 90
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v1
memory high gtpv1-arp 1

```

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 Resource Threshold Profile for 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 resource-threshold-profiles resource_v2 bearers-load low
percentage 60
set unified-edge cos-cac resource-threshold-profiles resource_v2 bearers-load low
gtpv2-priority-level 7
set unified-edge cos-cac resource-threshold-profiles resource_v2 bearers-load high
percentage 80
set unified-edge cos-cac resource-threshold-profiles resource_v2 bearers-load high
gtpv2-priority-level 4
set unified-edge cos-cac resource-threshold-profiles resource_v2 cpu low percentage 70
set unified-edge cos-cac resource-threshold-profiles resource_v2 cpu low
gtpv2-priority-level 7
set unified-edge cos-cac resource-threshold-profiles resource_v2 cpu high percentage 80
set unified-edge cos-cac resource-threshold-profiles resource_v2 cpu high
gtpv2-priority-level 4

```

```
set unified-edge cos-cac resource-threshold-profiles resource_v2 system-load low
percentage 85
set unified-edge cos-cac resource-threshold-profiles resource_v2 system-load low
gtpv2-priority-level 7
set unified-edge cos-cac resource-threshold-profiles resource_v2 system-load high
percentage 90
set unified-edge cos-cac resource-threshold-profiles resource_v2 system-load high
gtpv2-priority-level 4
set unified-edge cos-cac resource-threshold-profiles resource_v2 memory low percentage
85
set unified-edge cos-cac resource-threshold-profiles resource_v2 memory low
gtpv2-priority-level 10
set unified-edge cos-cac resource-threshold-profiles resource_v2 memory high percentage
90
set unified-edge cos-cac resource-threshold-profiles resource_v2 memory high
gtpv2-priority-level 5
```

**Step-by-Step
Procedure**

To configure resource threshold profiles for subscribers on a 4G network:

1. Configure the low and high thresholds for bearer load.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v2
bearers-load low percentage 60
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v2
bearers-load low gtpv2-priority-level 7
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v2
bearers-load high percentage 80
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v2
bearers-load high gtpv2-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_v2
cpu low percentage 70
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v2
cpu low gtpv2-priority-level 7
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v2
cpu high percentage 80
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v2
cpu high gtpv2-priority-level 4
```

3. Configure the low and high thresholds for the system load.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v2
system-load low percentage 85
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v2
system-load low gtpv2-priority-level 7
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v2
system-load high percentage 90
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v2
system-load high gtpv2-priority-level 4
```



NOTE: System load is an average of memory and CPU, so the values you specify for the system load should take into consideration values specified for the memory load and CPU load.

4. Configure the low and high thresholds for the memory load.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v2
memory low percentage 85
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v2
memory low gtpv2-priority-level 10
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v2
memory high percentage 90
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles resource_v2
memory high gtpv2-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 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 system_wide bearers-load low
percentage 60
set unified-edge cos-cac resource-threshold-profiles system_wide bearers-load low
gtpv2-priority-level 7
set unified-edge cos-cac resource-threshold-profiles system_wide bearers-load low
gtpv1-arp 2
set unified-edge cos-cac resource-threshold-profiles system_wide bearers-load high
percentage 80
set unified-edge cos-cac resource-threshold-profiles system_wide bearers-load high
gtpv2-priority-level 4
set unified-edge cos-cac resource-threshold-profiles system_wide bearers-load high
gtpv1-arp 1
set unified-edge cos-cac resource-threshold-profiles system_wide cpu low percentage 70
set unified-edge cos-cac resource-threshold-profiles system_wide cpu low
gtpv2-priority-level 7
set unified-edge cos-cac resource-threshold-profiles system_wide cpu low gtpv1-arp 2
set unified-edge cos-cac resource-threshold-profiles system_wide cpu high percentage
80
set unified-edge cos-cac resource-threshold-profiles system_wide cpu high
gtpv2-priority-level 5
set unified-edge cos-cac resource-threshold-profiles system_wide cpu high gtpv1-arp 1
set unified-edge cos-cac resource-threshold-profiles system_wide system-load low
percentage 85
```

```
set unified-edge cos-cac resource-threshold-profiles system_wide system-load low
  gtpv2-priority-level 7
set unified-edge cos-cac resource-threshold-profiles system_wide system-load low
  gtpv1-arp 2
set unified-edge cos-cac resource-threshold-profiles system_wide system-load high
  percentage 90
set unified-edge cos-cac resource-threshold-profiles system_wide system-load high
  gtpv2-priority-level 4
set unified-edge cos-cac resource-threshold-profiles system_wide system-load high
  gtpv1-arp 1
set unified-edge cos-cac resource-threshold-profiles system_wide memory low percentage
  85
set unified-edge cos-cac resource-threshold-profiles system_wide memory low
  gtpv2-priority-level 10
set unified-edge cos-cac resource-threshold-profiles system_wide memory low gtpv1-arp
  2
set unified-edge cos-cac resource-threshold-profiles system_wide memory high percentage
  90
set unified-edge cos-cac resource-threshold-profiles system_wide memory high
  gtpv2-priority-level 5
set unified-edge cos-cac resource-threshold-profiles system_wide memory high gtpv1-arp
  1
```

Step-by-Step Procedure

To configure a system-wide resource threshold profile:

1. Specify a name for the resource threshold profile and configure the low and high thresholds for bearer load.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles system_wide
  bearers-load low percentage 60
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles system_wide
  bearers-load low gtpv2-priority-level 7
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles system_wide
  bearers-load low gtpv1-arp 2
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles system_wide
  bearers-load high percentage 80
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles system_wide
  bearers-load high gtpv2-priority-level 4
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles system_wide
  bearers-load high gtpv1-arp 1
```

2. Configure the low and high thresholds for the CPU load.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles system_wide
  cpu low percentage 70
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles system_wide
  cpu low gtpv2-priority-level 7
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles system_wide
  cpu low gtpv1-arp 2
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles system_wide
  cpu high percentage 80
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles system_wide
  cpu high gtpv2-priority-level 5
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles system_wide
  cpu high gtpv1-arp 1
```

3. Configure the low and high thresholds for the system load.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles system_wide
system-load low percentage 85
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles system_wide
system-load low gtpv2-priority-level 7
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles system_wide
system-load low gtpv1-arp 2
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles system_wide
system-load high percentage 90
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles system_wide
system-load high gtpv2-priority-level 4
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles system_wide
system-load high gtpv1-arp 1
```



NOTE: System load is an average of the memory load and CPU load, so the values you specify for the system load should take into consideration values specified for the memory load and CPU load.

4. Configure the low and high thresholds for the memory load.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles system_wide
memory low percentage 85
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles system_wide
memory low gtpv2-priority-level 10
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles system_wide
memory low gtpv1-arp 2
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles system_wide
memory high percentage 90
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles system_wide
memory high gtpv2-priority-level 5
user@ggsn-pgw# set unified-edge cos-cac resource-threshold-profiles system_wide
memory high gtpv1-arp 1
```

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 maximum-bit-rate traffic-class
conversational both 3072
set unified-edge cos-cac cos-policy-profiles home_v1 maximum-bit-rate traffic-class
streaming both 2500
```

```
set unified-edge cos-cac cos-policy-profiles home_v1 maximum-bit-rate traffic-class
interactive both 896
set unified-edge cos-cac cos-policy-profiles home_v1 maximum-bit-rate traffic-class
background both 896
set unified-edge cos-cac cos-policy-profiles home_v1 maximum-bit-rate traffic-class
upgrade
set unified-edge cos-cac cos-policy-profiles home_v1 guaranteed-bit-rate traffic-class
conversational both 3008
set unified-edge cos-cac cos-policy-profiles home_v1 guaranteed-bit-rate traffic-class
streaming both 2372
set unified-edge cos-cac cos-policy-profiles home_v1 guaranteed-bit-rate traffic-class
upgrade
set unified-edge cos-cac cos-policy-profiles home_v1 violate-action transmit
set unified-edge cos-cac cos-policy-profiles home_v1 exceed-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, configure the maximum bit rate (MBR) for 3G subscriber traffic classes, and allow upgrade of PDP context requests with a lower MBR than the configured value.

[edit]
user@ggsn-pgw# set unified-edge cos-policy-profiles home_v1 maximum-bit-rate traffic-class conversational both 3072
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1 maximum-bit-rate traffic-class streaming both 2500
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1 maximum-bit-rate traffic-class interactive both 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1 maximum-bit-rate traffic-class background both 896
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1 maximum-bit-rate traffic-class upgrade
2. Configure the guaranteed bit rate (GBR) for 3G subscriber traffic and allow upgrade PDP context requests that specify a lower GBR than the configured value for a traffic class.

[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1 guaranteed-bit-rate traffic-class conversational both 3008
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1 guaranteed-bit-rate traffic-class streaming both 2372
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1 guaranteed-bit-rate traffic-class upgrade
3. Configure the action to take when the MBR for a PDP context request or the AMBR for a bearer request exceeds the configured value.

[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1 violate-action transmit
4. Configure the action to take when the GBR for a PDP context request exceeds the configured value.

[edit]


```
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v1
exceed-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 qos-class-identifier 5 upgrade
set unified-edge cos-cac cos-policy-profiles home_v2 allocation-retention-priority
  gtpv2-priority-value 5 upgrade
set unified-edge cos-cac cos-policy-profiles home_v2 aggregated-maximum-bit-rate
  downlink 2048
set unified-edge cos-cac cos-policy-profiles home_v2 aggregated-maximum-bit-rate
  uplink 2048
set unified-edge cos-cac cos-policy-profiles home_v2 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 profile, configure the highest QoS Class Identifier (QCI) that can be accepted, and allow upgrade of bearers with a lower QCI value than the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v2
  qos-class-identifier 5 upgrade
```

2. Configure ARP to only allow bearers with an ARP that is higher than or equal to the configured value when resources are limited.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v2
  allocation-retention-priority gtpv2-priority-value 4 upgrade
```

3. Configure the aggregate maximum bit rate (AMBR) for downlink and uplink traffic.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v2
  aggregated-maximum-bit-rate downlink 2048
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v2
  aggregated-maximum-bit-rate uplink 2048
```

4. Configure the action to take when the AMBR for a bearer request exceeds the configured value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles home_v2
  violate-action transmit
```



NOTE: The policer configuration specified in the home CoS policy profile also automatically determines the policer actions for visitor and roamer CoS policy profiles.

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 allocation-retention-priority
  gtpv1-priority-value 2
set unified-edge cos-cac cos-policy-profiles roamer_v1 maximum-bit-rate traffic-class
  conversational both 2500
set unified-edge cos-cac cos-policy-profiles roamer_v1 maximum-bit-rate traffic-class
  streaming both 2048
set unified-edge cos-cac cos-policy-profiles roamer_v1 maximum-bit-rate traffic-class
  interactive both 896
set unified-edge cos-cac cos-policy-profiles roamer_v1 maximum-bit-rate traffic-class
  background both 768
set unified-edge cos-cac cos-policy-profiles roamer_v1 guaranteed-bit-rate traffic-class
  conversational both 2372
set unified-edge cos-cac cos-policy-profiles roamer_v1 guaranteed-bit-rate traffic-class
  streaming both 1984
```

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 and configure the ARP to only allow bearers with an ARP that is higher than or equal to the configured value when resources are limited.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
  allocation-retention-priority gtpv1-priority-value 2
```

2. Configure the MBR for 3G subscriber traffic classes.

```
[edit]
user@ggsn-pgw# set unified-edge cos-policy-profiles roamer_v1 maximum-bit-rate
  traffic-class conversational both 2500
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
  maximum-bit-rate traffic-class streaming both 2048
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
  maximum-bit-rate traffic-class interactive both 896
```

```
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
maximum-bit-rate traffic-class background both 768
```

3. Configure the GBR for 3G subscriber traffic.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
guaranteed-bit-rate traffic-class conversational both 2372
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v1
guaranteed-bit-rate traffic-class streaming both 1984
```



NOTE: The policer configuration specified in the home CoS policy profile determines the actions for visitor and roamer CoS policy profiles.

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 qos-class-identifier 7
set unified-edge cos-cac cos-policy-profiles roamer_v2 allocation-retention-priority
gtpv2-priority-value 9
set unified-edge cos-cac cos-policy-profiles roamer_v2 aggregated-maximum-bit-rate
downlink 1600
set unified-edge cos-cac cos-policy-profiles roamer_v2 aggregated-maximum-bit-rate
uplink 1600
set unified-edge cos-cac cos-policy-profiles roamer_v2 aggregated-maximum-bit-rate
downgrade
set unified-edge cos-cac cos-policy-profiles roamer_v2 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 profile and configure the highest QCI that can be accepted.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v2
qos-class-identifier 7
```

2. Configure ARP to only allow bearers with an ARP that is higher than or equal to the configured value when resources are limited.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v2
allocation-retention-priority gtpv2-priority-value 9
```

3. Configure the AMBR for downlink and uplink traffic.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v2
  aggregated-maximum-bit-rate downlink 1600
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v2
  aggregated-maximum-bit-rate uplink 1600
```

4. Downgrade bearer requests that specify a higher AMBR than the configured AMBR value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles roamer_v2
  aggregated-maximum-bit-rate downgrade
```



NOTE: The policer configuration specified in the home CoS policy profile determines the actions for visitor and roamer CoS policy profiles.

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 in 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 allocation-retention-priority
  gtpv1-priority-value 2
set unified-edge cos-cac cos-policy-profiles visitor_v1 maximum-bit-rate traffic-class
  conversational both 2048
set unified-edge cos-cac cos-policy-profiles visitor_v1 maximum-bit-rate traffic-class
  streaming both 1472
set unified-edge cos-cac cos-policy-profiles visitor_v1 maximum-bit-rate traffic-class
  interactive both 768
set unified-edge cos-cac cos-policy-profiles visitor_v1 maximum-bit-rate traffic-class
  background both 576
set unified-edge cos-cac cos-policy-profiles visitor_v1 guaranteed-bit-rate traffic-class
  conversational both 1984
set unified-edge cos-cac cos-policy-profiles visitor_v1 guaranteed-bit-rate traffic-class
  streaming 1408
```

Step-by-Step Procedure To configure a CoS policy profile for visiting subscribers in a 3G network:

1. Specify a name for the CoS policy profile and configure the ARP to only allow bearers with an ARP that is higher than or equal to the configured value when resources are limited.

```
[edit]
```

```
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
gtpv1-priority-value 2
```

2. Configure the MBR for 3G subscriber traffic classes.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
maximum-bit-rate traffic-class conversational both 2048
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
maximum-bit-rate traffic-class streaming both 1472
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
maximum-bit-rate traffic-class interactive both 768
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
maximum-bit-rate traffic-class background both 576
```

3. Configure the GBR for 3G subscriber traffic.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
guaranteed-bit-rate traffic-class conversational both 1984
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v1
guaranteed-bit-rate traffic-class streaming 1408
```



NOTE: The policer configuration specified in the home CoS policy profile determines the actions for visitor and roamer CoS policy profiles.

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 in 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 qos-class-identifier 5
set unified-edge cos-cac cos-policy-profiles visitor_v2 allocation-retention-priority
gtpv2-priority-value 9
set unified-edge cos-cac cos-policy-profiles visitor_v2 aggregated-maximum-bit-rate
downlink 1600
set unified-edge cos-cac cos-policy-profiles visitor_v2 aggregated-maximum-bit-rate
uplink 1600
set unified-edge cos-cac cos-policy-profiles visitor_v2 aggregated-maximum-bit-rate
downgrade
```

Step-by-Step Procedure To configure a CoS policy profile for visiting subscribers in a 4G network:

1. Specify a name for the CoS profile and configure the highest QCI that can be accepted.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v2
qos-class-identifier 5
```

2. Configure ARP to only allow bearers with an ARP that is higher than or equal to the configured value when resources are limited.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v2
allocation-retention-priority gtpv2-priority-value 9
```

3. Configure the AMBR for downlink and uplink traffic.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v2
aggregated-maximum-bit-rate downlink 1024
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v2
aggregated-maximum-bit-rate uplink 1024
```

4. Reject bearer requests that specify a higher AMBR than the configured AMBR value.

```
[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles visitor_v2
aggregated-maximum-bit-rate reject
```



NOTE: The policer configuration specified in the home CoS policy profile determines the actions for visitor and roamer CoS policy profiles.

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 aggregated-maximum-bit-rate
both 1024
set unified-edge cos-cac cos-policy-profiles system_wide maximum-bit-rate traffic-class
conversational both 512
set unified-edge cos-cac cos-policy-profiles system_wide maximum-bit-rate traffic-class
streaming both 256
set unified-edge cos-cac cos-policy-profiles system_wide maximum-bit-rate traffic-class
interactive both 128
set unified-edge cos-cac cos-policy-profiles system_wide maximum-bit-rate traffic-class
background both 64
set unified-edge cos-cac cos-policy-profiles system_wide guaranteed-bit-rate traffic-class
conversational both 512
```

```

set unified-edge cos-cac cos-policy-profiles system_wide guaranteed-bit-rate traffic-class
streaming both 256
set unified-edge cos-cac cos-policy-profiles system_wide violate-action transmit
set unified-edge cos-cac cos-policy-profiles system_wide exceed-action transmit

```

Step-by-Step Procedure

To configure a system-level CoS policy profile for 3G and 4G subscribers:

1. Specify a name for the CoS profile and configure the AMBR for 4G subscriber traffic.

```

[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
aggregated-maximum-bit-rate both 1024

```

2. Configure the MBR for 3G subscriber traffic classes.

```

[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
maximum-bit-rate traffic-class conversational both 512
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
maximum-bit-rate traffic-class streaming both 256
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
maximum-bit-rate traffic-class interactive both 128
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
maximum-bit-rate traffic-class background both 64

```

3. Configure the GBR for 3G subscriber traffic classes.

```

[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
guaranteed-bit-rate traffic-class conversational both 512
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
guaranteed-bit-rate traffic-class streaming both 256

```

4. Configure the action to take when the MBR for a PDP context request or the AMBR for a bearer request exceeds the configured value.

```

[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
violate-action transmit

```

5. Configure the action to take when the GBR for a PDP context request exceeds the configured value.

```

[edit]
user@ggsn-pgw# set unified-edge cos-cac cos-policy-profiles system_wide
exceed-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 bandwidth-pools bw_pool_uplink
```

2. Specify a name for the downlink bandwidth pool.

```
[edit ]
user@host# edit unified-edge cos-cac 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. Allocate bandwidth from the bandwidth pool to the conversational and streaming traffic classes as a percentage of the total bandwidth for the pool:

- a. Allocate a percentage of the total bandwidth to reserve for the conversational traffic class.

```
[edit]
user@host# set unified-edge cos-cac bandwidth-pools bw_pool_uplink
traffic-class conversational percentage 35
user@host# set unified-edge cos-cac bandwidth-pools bw_pool_downlink
traffic-class conversational percentage 35
```

- b. Allocate the percentage of the total bandwidth to be reserved for the streaming traffic class.

```
[edit]
user@host# set unified-edge cos-cac bandwidth-pools bw_pool_uplink
traffic-class streaming percentage 20
user@host# set unified-edge cos-cac bandwidth-pools bw_pool_downlink
traffic-class streaming percentage 20
```

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_v1
set unified-edge local-policies local_v1 classifier-profile home_v1
set unified-edge local-policies local_v1 cos-policy-profile home_v1
```



```

set unified-edge local-policies local_v1 roamer-classifier-profile roamer_v1
set unified-edge local-policies local_v1 roamer-cos-policy-profile roamer_v1
set unified-edge local-policies local_v1 visitor-classifier-profile visitor_v1
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_v1

```

3. Specify the classifier profiles for the local policy to define the mapping of traffic classes and QoS Class Identifiers to a forwarding class and loss priority.

```

[edit]
user@ggsn-pgw# set unified-edge local-policies local_v1 classifier-profile home_v1
user@ggsn-pgw# set unified-edge local-policies local_v1 roamer-classifier-profile roamer_v1
user@ggsn-pgw# set unified-edge local-policies local_v1 visitor-classifier-profile visitor_v1

```

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_v2
set unified-edge local-policies local_v2 classifier-profile home_v2
set unified-edge local-policies local_v2 cos-policy-profile home_v2
set unified-edge local-policies local_v2 roamer-classifier-profile roamer_v2
set unified-edge local-policies local_v2 roamer-cos-policy-profile roamer_v2
set unified-edge local-policies local_v2 visitor-classifier-profile visitor_v2
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_v2
```

3. Specify the classifier profiles for the local policy to define the mapping of QoS Class Identifiers to a forwarding class and loss priority.

```
[edit]
user@ggsn-pgw# set unified-edge local-policies local_v2 classifier-profile home_v2
user@ggsn-pgw# set unified-edge local-policies local_v2 roamer-classifier-profile
roamer_v2
user@ggsn-pgw# set unified-edge local-policies local_v2 visitor-classifier-profile
visitor_v2
```

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_system
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_system
```

3. Specify the classifier profile for the local policy to define the mapping of traffic classes and Qos Class Identifiers to a forwarding class and loss priority.

```
[edit]
```

```
user@ggsn-pgw# set unified-edge local-policies local_system_wide classifier-profile
system_wide
```

- 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
```

- Specify a bandwidth pool for downlink traffic.

```
[edit ]
user@host# set unified-edge local-policies local_system_wide dl-bandwidth-pool
bw_pool_downlink
```

- 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.

- At the gateway level, apply the system-wide local policy.

```
[edit]
user@host# set gateways ggsn-pgw MBG1 local-policy-profile local_system_wide
```

- 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 dscp4_ingress_rw]
[set class-of-service rewrite-rules dscp dscp4_ingress_rw forwarding class af1 loss-priority
  high code-point 001110]
[set class-of-service rewrite-rules dscp dscp4_ingress_rw forwarding class af1 loss-priority
  low code-point 001010]
[set class-of-service rewrite-rules dscp dscp4_ingress_rw forwarding class af2 loss-priority
  high code-point 010110]
[set class-of-service rewrite-rules dscp dscp4_ingress_rw forwarding class af2 loss-priority
  low code-point 010010]
[set class-of-service rewrite-rules dscp dscp4_ingress_rw forwarding class af3 loss-priority
  high code-point 011110]
[set class-of-service rewrite-rules dscp dscp4_ingress_rw forwarding class af3 loss-priority
  low code-point 011010]
[set class-of-service rewrite-rules dscp dscp4_ingress_rw forwarding class af4 loss-priority
  high code-point 100110]
[set class-of-service rewrite-rules dscp dscp4_ingress_rw forwarding class af4 loss-priority
  low code-point 100010]
```

Step-by-Step Procedure To configure the ingress rewrite rules for IPv4 packets:

1. Specify a name for the ingress rewrite rules.


```
[edit]
user@host# edit class-of-service rewrite-rules dscp dscp4_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 dscp4_ingress_rw forwarding
  class af1 loss-priority high code-point 001110
user@host# set class-of-service rewrite-rules dscp dscp4_ingress_rw forwarding
  class af1 loss-priority low code-point 001010
user@host# set class-of-service rewrite-rules dscp dscp4_ingress_rw forwarding
  class af2 loss-priority high code-point 010110
user@host# set class-of-service rewrite-rules dscp dscp4_ingress_rw forwarding
  class af2 loss-priority low code-point 010010
user@host# set class-of-service rewrite-rules dscp dscp4_ingress_rw forwarding
  class af3 loss-priority high code-point 011110
user@host# [set class-of-service rewrite-rules dscp dscp4_ingress_rw forwarding
  class af3 loss-priority low code-point 011010
user@host# [set class-of-service rewrite-rules dscp dscp4_ingress_rw forwarding
  class af4 loss-priority high code-point 100110
user@host# [set class-of-service rewrite-rules dscp dscp4_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 dscp_v6_ingress_rw]
[set class-of-service rewrite-rules dscp dscp_v6_ingress_rw forwarding class af1 loss-priority
  high code-point 001110]
[set class-of-service rewrite-rules dscp dscp_v6_ingress_rw forwarding class af1 loss-priority
  low code-point 001010]
[set class-of-service rewrite-rules dscp dscp_v6_ingress_rw forwarding class af2 loss-priority
  high code-point 010110]
[set class-of-service rewrite-rules dscp dscp_v6_ingress_rw forwarding class af2 loss-priority
  low code-point 010010]
[set class-of-service rewrite-rules dscp dscp_v6_ingress_rw forwarding class af3 loss-priority
  high code-point 011110]
[set class-of-service rewrite-rules dscp dscp_v6_ingress_rw forwarding class af3 loss-priority
  low code-point 011010]
[set class-of-service rewrite-rules dscp dscp_v6_ingress_rw forwarding class af4 loss-priority
  high code-point 100110]
[set class-of-service rewrite-rules dscp dscp_v6_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 dscp_v6_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 dscp_v6_ingress_rw forwarding
  class af1 loss-priority high code-point 001110
user@host# set class-of-service rewrite-rules dscp dscp_v6_ingress_rw forwarding
  class af1 loss-priority low code-point 001010
user@host# set class-of-service rewrite-rules dscp dscp_v6_ingress_rw forwarding
  class af2 loss-priority high code-point 010110
user@host# set class-of-service rewrite-rules dscp dscp_v6_ingress_rw forwarding
  class af2 loss-priority low code-point 010010
user@host# set class-of-service rewrite-rules dscp dscp_v6_ingress_rw forwarding
  class af3 loss-priority high code-point 011110
user@host# [set class-of-service rewrite-rules dscp dscp_v6_ingress_rw forwarding
  class af3 loss-priority low code-point 011010]
user@host# [set class-of-service rewrite-rules dscp dscp_v6_ingress_rw forwarding
  class af4 loss-priority high code-point 100110]
user@host# [set class-of-service rewrite-rules dscp dscp_v6_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 dscp_v6_egress_rw]
[set class-of-service rewrite-rules dscp-ipv6 dscp_v6_egress_rw forwarding class af1
loss-priority high code-point 001110]
```

```
[set class-of-service rewrite-rules dscp-ipv6 dscp6_egress_rw forwarding class af1
loss-priority low code-point 001010]
[set class-of-service rewrite-rules dscp-ipv6 dscp6_egress_rw forwarding class af2
loss-priority high code-point 010110]
[set class-of-service rewrite-rules dscp-ipv6 dscp6_egress_rw forwarding class af2
loss-priority low code-point 010010]
[set class-of-service rewrite-rules dscp-ipv6 dscp6_egress_rw forwarding class af3
loss-priority high code-point 011110]
[set class-of-service rewrite-rules dscp-ipv6 dscp6_egress_rw forwarding class af3
loss-priority low code-point 011010]
[set class-of-service rewrite-rules dscp-ipv6 dscp6_egress_rw forwarding class af4
loss-priority high code-point 100110]
[set class-of-service rewrite-rules dscp-ipv6 dscp6_egress_rw forwarding class af4
loss-priority low code-point 100010]
[set class-of-service rewrite-rules dscp-ipv6 dscp6_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.

[edit]
user@host# edit class-of-service rewrite-rules dscp-ipv6 dscp6_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-ipv6 dscp6_egress_rw
forwarding class af1 loss-priority high code-point 001110
user@host# set class-of-service rewrite-rules dscp-ipv6 dscp6_egress_rw
forwarding class af1 loss-priority low code-point 001010
user@host# [set class-of-service rewrite-rules dscp-ipv6 dscp6_egress_rw
forwarding class af2 loss-priority high code-point 010110
user@host# set class-of-service rewrite-rules dscp-ipv6 dscp6_egress_rw
forwarding class af2 loss-priority low code-point 010010
user@host# set class-of-service rewrite-rules dscp-ipv6 dscp6_egress_rw
forwarding class af3 loss-priority high code-point 011110
user@host# set class-of-service rewrite-rules dscp-ipv6 dscp6_egress_rw
forwarding class af3 loss-priority low code-point 011010
user@host# set class-of-service rewrite-rules dscp-ipv6 dscp6_egress_rw
forwarding class af4 loss-priority high code-point 100110
user@host# set class-of-service rewrite-rules dscp-ipv6 dscp6_egress_rw
forwarding class af4 loss-priority low code-point 100010
user@host# set class-of-service rewrite-rules dscp-ipv6 dscp6_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 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
dscpv6_egress_rw protocol gtp-inet-both
```

```
[edit]
```

```
user@host# set class-of-service interfaces mif unit 1 rewrite-rules dscp
dscpv4_egress_rw protocol gtp-inet-both
```

```
user@host# set class-of-service interfaces mif unit 1 rewrite-rules dscp
dscpv6_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
dscpv4_egress_rw protocol gtp-inet-both
```

```
user@host# set class-of-service interfaces mif unit 1 rewrite-rules dscp
dscpv6_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 381
- [Display 4G Subscriber Information for Traffic Marked with a Specified QoS Class Identifier](#) on page 382
- [Display 3G Subscriber Information for Traffic Marked with the Specified Traffic Class](#) on page 382
- [Display the Requested and Negotiated QoS Parameters for Mobile Subscribers](#) on page 383

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 qos 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 QoS Class Identifier

Purpose Verify that the QoS configuration is working properly for 4G subscribers by showing statistics for subscriber packets with a specified QoS class identifier.

Action

```
user@host> show unified-edge ggsn-pgw qos 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 qos 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 310](#)
- [Call Admission Control Overview on page 315](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 317](#)
- [Policing Subscriber Traffic on the Broadband Gateway Overview on page 318](#)
- [Configuring QoS on the Broadband Gateway Overview on page 323](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

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 310](#)
- [Call Admission Control Overview on page 315](#)
- [Example: Configuring QoS and CAC on a S-GW on page 385](#)

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 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 DCSP 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 385](#)
- [Overview on page 386](#)
- [Configuration on page 386](#)

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 386](#)
- [Configuring the IPv4 Interfaces on page 387](#)
- [Configuring the QoS and CAC classifier and resource threshold profiles and parameters on page 387](#)
- [Configuring S-GW CAC parameters on page 388](#)
- [Configuring Forwarding Classes and Rewrite Rules on page 389](#)
- [Apply the Rewrite Rule for Ingress \(S5\) and Egress \(S11\) on page 390](#)

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 172.16.1/24
```

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

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 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
```

**Step-by-Step
Procedure**

To configure the QoS and CAC classifier and resource threshold profiles and parameters:

1. Configure classifier profile `classifier_v2`.

```
[edit]
user@sgw1# edit unified-edge cos-cac classifier-profiles classifier_v2
```
2. Specify the QoS parameters for `af1` and `af3`.

```
[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
```
3. Configure resource threshold profile `resource_v2`.

```
[edit]
user@sgw1# edit unified-edge cos-cac resource-threshold-profiles resource_v2
```
4. 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
```
5. Configure the local policy `local_profile_v2`.

```
[edit]
user@sgw1# edit unified-edge local-policies local_profile_v2
```
6. 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:

1. 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

```

2. 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 310](#)
- [Call Admission Control Overview on page 315](#)
- [Configuring S-GW-Specific CAC Parameters on page 384](#)

PART 8

Maintenance

- [Maintenance Mode on page 393](#)

CHAPTER 13

Maintenance Mode

- [Mobility Maintenance Mode Overview on page 394](#)
- [Changing a GTP Interface Address on page 395](#)
- [Deleting a GTP Interface on page 396](#)
- [Modifying an Access Point Name on page 398](#)
- [Configuring the Mobile Interface of an Access Point Name on page 399](#)
- [Deleting an Access Point Name on page 401](#)
- [Changing a Charging Profile on page 402](#)
- [Changing a Transport Profile on page 403](#)
- [Changing a Trigger Profile on page 405](#)
- [Deleting a Charging Profile on page 406](#)
- [Changing a Call Detail Record Profile in a Charging Profile on page 407](#)
- [Changing Address Attributes in the Mobile Address Pool on page 408](#)
- [Deleting a Mobile Address Pool on page 410](#)
- [Example: Changing Access Point Name Values on page 411](#)
- [Example: Deleting an APN on page 412](#)
- [Example: Changing a Charging Profile on page 413](#)
- [Example: Changing a Transport Profile on page 415](#)
- [Example: Changing Mobility Pool Attributes on page 416](#)
- [Example: Deleting a Mobility Address Pool on page 422](#)
- [Example: Modifying Mobile Interface Parameters on page 423](#)

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 can 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 a charging profile.
- Delete or modify a charging data record (CDR) profile or CDR type.
- Delete or modify a transport profile.
- Delete or modify a trigger 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. This is logical—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 Address on page 395](#)
- [Deleting a GTP Interface on page 396](#)
- [Modifying an Access Point Name on page 398](#)
- [Configuring the Mobile Interface of an Access Point Name on page 399](#)
- [Deleting an Access Point Name on page 401](#)
- [Changing a Charging Profile on page 402](#)
- [Deleting a Charging Profile on page 406](#)
- [Changing a Transport Profile on page 403](#)

Changing a GTP Interface Address

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 394](#)
- [Deleting a GTP Interface on page 396](#)

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 394](#)
- [Changing a GTP Interface Address on page 395](#)

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 394](#)
- [Configuring the Mobile Interface of an Access Point Name on page 399](#)
- [Deleting an Access Point Name on page 401](#)

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.

8. Exit maintenance mode.

```
user@host# delete unified-edge gateways ggsn-pgw gw-name apn-services apns apn-name service-mode
user@host# commit
```

9. Verify that changes were properly committed.

```
user@host# run show configuration unified-edge gateways ggsn-pgw gw-name apn-services apns apn-name
```

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 394](#)
- [Example: Changing Access Point Name Values on page 411](#)
- [Deleting an Access Point Name on page 401](#)

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:

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 apn apn-name
service-mode maintenance
user@host# commit
```

3. 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).

4. Verify that there are no subscribers active on the APN.

```
user@host# run show unified-edge ggsn-pgw apn apn-name gateway gw-name
```

5. (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 394](#)
- [Configuring the Mobile Interface of an Access Point Name on page 399](#)
- [Example: Changing Access Point Name Values on page 411](#)

Changing a Charging Profile

This procedure describes how to use maintenance mode to change a charging profile. You must first halt new sessions from being started and verify that there are no active sessions remaining.

You can make the following types of changes to the charging profile in maintenance mode:

- CDR profile
- Transport profile
- Trigger profile

To change the charging profile:

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  
user@host# commit
```

3. Verify that the charging gateway is in maintenance mode.

```
user@host# show unified-edge ggsn-pgw subscribers charging charging-profile  
profile-name gateway gw-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 there are some sessions 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).

Verify that there are no subscribers active on this charging profile.

```
user@host# show unified-edge ggsn-pgw subscribers charging charging-profile  
profile-name
```

4. (Optional) Terminate subscribers using a charging profile using the **clear** command.


```
user@host# run clear unified-edge ggsn-pgw subscribers charging charging-profile
profile-name gateway gw-name
```

5. 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.



NOTE: These modifications must be made in active maintenance mode or they will fail.

6. Make the changes and verify that they were properly committed.

```
user@host# show unified-edge ggsn-pgw subscribers charging charging-profile
profile-name gateway gw-name
```

7. 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
```

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 394](#)
- [Changing a Transport Profile on page 403](#)
- [Changing a Trigger Profile on page 405](#)
- [Deleting a Charging Profile on page 406](#)
- [Changing a Call Detail Record Profile in a Charging Profile on page 407](#)

Changing a Transport Profile

This procedure describes how to use maintenance mode to change a transport profile. You must first halt new sessions from being started and verify that there are no active sessions remaining.

To change a transport profile:

1. Enter configuration mode in the CLI.

```
user@host> configure
```

2. Activate maintenance mode for a charging 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 charging gateway is in maintenance mode.

```
user@host# run show unified-edge ggsn-pgw charging service-mode transport-profile
profile-name gateway gw-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 there are some sessions 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 subscribers active on this charging profile.

```
user@host# run show unified-edge ggsn-pgw subscribers charging transport-profile  
profile-name gateway gw-name
```

5. (Optional) Terminate sessions using the **clear** command.

```
user@host# run clear unified-edge ggsn-pgw subscribers charging transport-profile  
profile-name gateway gw-name
```

6. When the subscriber count is zero and all sessions have ended, you can make and commit changes to the charging transport profile in active maintenance mode.



NOTE: These modifications must be made in active maintenance mode or they will fail.

7. Modify the charging transport profile as required.

8. Exit maintenance mode and commit.

```
user@host# delete unified-edge gateways ggsn-pgw gw-name charging  
transport-profile profile-name service-mode commit
```

9. Verify that changes were properly committed.

```
user@host# run show configuration unified-edge ggsn-pgw gateway gw-name
```

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 394](#)
- [Changing a Charging Profile on page 402](#)
- [Changing a Trigger Profile on page 405](#)
- [Deleting a Charging Profile on page 406](#)
- [Changing a Call Detail Record Profile in a Charging Profile on page 407](#)

Changing a Trigger Profile

This procedure describes how to use maintenance mode to change a trigger profile. You must first halt new sessions from being started and verify that there are no active sessions remaining.

To change a trigger profile:

1. Enter configuration mode in the CLI.

```
user@host> configure
```

2. Activate maintenance mode for a charging trigger profile:

```
user@host# set unified-edge gateways ggsn-pgw gw-name charging trigger-profiles
profile-name service-mode maintenance
user@host# commit
```

3. Verify that the charging gateway is in maintenance mode.

```
user@host# run show unified-edge ggsn-pgw charging service-mode trigger-profile
profile-name gateway gw-name
```

Verify that there are no subscribers active on this charging profile.

```
user@host# run show unified-edge ggsn-pgw subscribers charging trigger-profile
profile-name gateway gw-name
```

4. (Optional) Terminate sessions using the **clear** command

```
user@host# run clear unified-edge ggsn-pgw subscribers charging trigger-profile
profile-name gateway gw-name
```

5. When the subscriber count for the charging profile and all CDRs generated for the charging profile is zero, you can make and commit changes to the charging trigger profile in active maintenance mode.



NOTE: These modifications must be made in active maintenance mode or they will fail.

6. Modify the charging trigger profile.

7. Commit your changes and exit maintenance mode.

```
user@host# delete unified-edge gateways ggsn-pgw gw-name charging trigger-profile
profile-name service-mode commit
```

8. Verify that changes were properly committed.

```
user@host# run show configuration unified-edge ggsn-pgw gateway gw-name
```

9. 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 394](#)
- [Changing a Charging Profile on page 402](#)

- [Changing a Transport Profile on page 403](#)
- [Deleting a Charging Profile on page 406](#)
- [Changing a Call Detail Record Profile in a Charging Profile on page 407](#)

Deleting a Charging Profile

This procedure describes how to use maintenance mode to delete a charging profile. You must first halt new sessions from being started and verify that there are no active sessions remaining.

The example shown is for deleting a charging transport profile. The same configuration applies for deleting a transport or trigger profile.



NOTE: Use this procedure to delete a charging profile or a charging transport profile. To specify a charging profile, replace the syntax `charging transport-profiles` with `charging charging-profiles`.

To delete a charging profile:

1. Enter configuration mode in the CLI.

```
user@host> configure
```

2. Activate maintenance mode for a charging 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 charging gateway is in maintenance mode.

```
user@host# show unified-edge ggsn-pgw charging service-mode transport-profile  
profile-name gateway gw-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 there are some sessions 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 subscribers active on this charging profile.

```
user@host# show unified-edge ggsn-pgw charging service-mode transport-profile  
profile-name gateway gw-name
```

5. (Optional) Terminate sessions that are using a charging profile using the `clear` command.

```
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 charging profile attributes in active maintenance mode.



NOTE: These modifications must be made in active maintenance mode or they will fail.

- Delete the charging transport profile, commit your changes, and exit maintenance mode.

```
user@host# delete unified-edge gateways ggsn-pgw gw-name charging
transport-profile profile-name service-mode
user@host# commit
```

- Verify that changes were properly committed.

```
user@host# run show configuration unified-edge ggsn-pgw gateway gw-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 394](#)
- [Changing a Charging Profile on page 402](#)
- [Changing a Transport Profile on page 403](#)
- [Changing a Trigger Profile on page 405](#)
- [Changing a Call Detail Record Profile in a Charging Profile on page 407](#)

Changing a Call Detail Record Profile in a Charging Profile

This procedure describes how to use maintenance mode to change a CDR profile in a charging profile. You must first halt new sessions from being started and verify that there are no active sessions remaining.

To make changes to a CDR profile in a charging profile in maintenance mode:

- Enter configuration mode in the CLI.

```
user@host> configure
```

- Place the charging profile in maintenance mode.

```
user@host# set unified-edge gateways ggsn-pgw gw-name charging charging-profiles
profile-name maintenance mode
user@host# commit
```

- Verify that, for this charging profile, no subscribers are active and that the CDRs have been flushed.

```
user@host# run show unified-edge ggsn-pgw gw-name subscribers charging
charging-profile profile-name
```

4. (Optional) Terminate sessions that are using a mobile pool using the **clear** command.

```
user@host# run clear unified-edge ggsn-pgw subscribers charging charging-profile  
profile-name
```

5. When the subscriber count is zero and all sessions have ended, maintenance mode is active. You can make and commit changes to pool attributes in active maintenance mode.



NOTE: These modifications must be made in active maintenance mode or they will fail.

6. Make the changes and verify that they were properly committed.

```
user@host# run show unified-edge ggsn-pgw subscribers charging charging-profile  
profile-name gateway gw-name charging charging-profile profile-name
```

7. Commit your changes and exit maintenance mode 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
```

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 394](#)
- [Changing a Charging Profile on page 402](#)
- [Changing a Transport Profile on page 403](#)
- [Changing a Trigger Profile on page 405](#)
- [Deleting a Charging Profile on page 406](#)

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 394](#)
- [Deleting a Mobile Address Pool on page 410](#)

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 408](#)

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 394](#)
 - [Changing Address Attributes in the Mobile Address Pool on page 408](#)

Example: Changing Access Point Name Values

- [Requirements on page 411](#)
- [Overview on page 411](#)
- [Configuration on page 411](#)

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 394](#)
- [Modifying an Access Point Name on page 398](#)

Example: Deleting an APN

- [Requirements on page 412](#)
- [Overview on page 412](#)
- [Configuration on page 412](#)

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
```

- 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.

- Delete the APN named Central and commit the changes.

```
user@host# delete unified-edge ggsn-pgw MBG1 apn-services apnsCentral
user@host# commit
```

- Exit maintenance mode and commit.

```
user@host# delete unified-edge ggsn-pgw MBG1 apn-services apns Central
service-mode
user@host# commit
```

- 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.

- 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 394](#)
- [Deleting an Access Point Name on page 401](#)

Example: Changing a Charging Profile

This example shows how to change a charging profile using maintenance mode.

- [Requirements on page 413](#)
- [Overview on page 414](#)
- [Configuration on page 414](#)

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 charging profile attributes without affecting mobility subscribers using other charging profiles.

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 Service Mode Status
```

```
Gateway Name : MBG1
...
Profile Name : juniper
Service Mode : Operational
```

2. Place the MX Series router 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 Service Mode Status
```

```
Gateway Name : MBG1
...
Profile Name : Service Mode
juniper : Maintenance - Active Phase
```

6. 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
```

7. Return the gateway to operational state.

```
user@host# run show unified-edge ggsn-pgw gateway service-mode
```

Results The charging profile is in active maintenance mode. You can change profile attributes and commit them.

Related Documentation

- [Mobility Maintenance Mode Overview on page 394](#)
- [Changing a Charging Profile on page 402](#)

Example: Changing a Transport Profile

This example shows how to change a transport profile using maintenance mode.

- [Requirements on page 415](#)
- [Overview on page 415](#)
- [Configuration on page 415](#)

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 transport profile attributes without affecting mobility subscribers using other transport profiles.

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 Service Mode Status
```

```
Gateway Name   : MBG1
...
Profile Name   : trans_p
Service Mode   : Operational
```

2. Set the MX Series router 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 maintenance mode
```

```
Gateway Name   : MBG1
...
Profile Name   : Service Mode
trans_p       : Maintenance - Active Phase
```

6. 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
```

7. Return the gateway to operational state.

```
user@host# run show unified-edge ggsn-pgw gateway service-mode
```

Results The transport profile is in active maintenance mode. You can change profile attributes and commit them.

Related Documentation

- [Mobility Maintenance Mode Overview on page 394](#)
- [Changing a Transport Profile on page 403](#)

Example: Changing Mobility Pool Attributes

- [Requirements on page 416](#)
- [Overview on page 416](#)
- [Configuration on page 416](#)

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 394](#)
- [Changing Address Attributes in the Mobile Address Pool on page 408](#)

Example: Deleting a Mobility Address Pool

- [Requirements on page 422](#)
- [Example of Deleting a Mobility Address Pool on page 422](#)
- [Configuration on page 422](#)

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 394](#)
 - [Deleting a Mobile Address Pool on page 410](#)

Example: Modifying Mobile Interface Parameters

- [Requirements on page 424](#)
- [Overview on page 424](#)
- [Configuration on page 424](#)

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 424](#)
- [Changing the Mobile Interface for an Access Point Name \(APN\) on page 425](#)

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: Sendbcast-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;
}
anonymous-user {
    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 394](#)
- [Deleting a Mobile Address Pool on page 410](#)

PART 9

Monitoring and Troubleshooting

- [Monitoring on page 429](#)
- [Troubleshooting on page 457](#)

CHAPTER 14

Monitoring

- [Monitoring the Mobile Environment - Key Performance Indicators on page 429](#)
- [Monitoring Resources on page 430](#)
- [Monitoring GTP Signaling on page 430](#)
- [Monitoring Session Status on page 431](#)
- [Monitoring CPU Indicators on page 432](#)
- [Monitoring Memory Indicators on page 433](#)
- [Monitoring Charging Gateways on page 433](#)
- [Monitoring Data Path Measurements on page 435](#)
- [Monitoring Call Rate Statistics on page 435](#)
- [Monitoring Data Rate Statistics on page 435](#)
- [Tracing Control Packets on page 438](#)
- [How to Trace Data Packets from Gn to Gi Interfaces on page 442](#)
- [Trace Data Packets from Gi to Gn Interfaces on page 446](#)
- [How to Verify Charging Statistics Processing on page 453](#)

Monitoring the Mobile Environment - Key Performance Indicators

This topic describes the most common key performance indicators that you can use to determine the health of the Junos Mobility environment.

These key performance indicators include:

- GTP signaling statistics
- Session status indicators
- CPU utilization indicators
- Memory utilization indicators
- Monitored resource usage indicators (Address pools, system/APN bandwidth usage, Packet Forwarding Engine load, and so on)
- AAA authentication or accounting metrics
- Charging gateway status, congestion indicators with round trip time calculations

- Data path measurements
- Per server statistics for AAA, GTP, and CG
- Data rate measurements per configured interval

**Related
Documentation**

- [Monitoring Data Rate Statistics on page 435](#)
- [Monitoring Data Path Measurements on page 435](#)
- [Monitoring Session Status on page 431](#)
- [Monitoring GTP Signaling on page 430](#)

Monitoring Resources

To avoid overload conditions, monitor the following resources:

- Detailed control plane snapshot of number of bearers per state
- Number of bearers waiting for authentication, address allocation, data path setup, and so on
- CPU of each session PIC
- Memory consumed on each session PIC
- Maximum bearer limit
- Anchor Packet Forwarding Engine load
- Individual session PIC average load
- System data path bandwidth for assured quality of service
- Queue depths (AAA, charging, GTP input, and so on)
- External interfaces like RADIUS Charging Gateway by tracking success/fail, monitoring round trip time, and so on
- Internal resource usage for local pool addresses available and so on

Monitoring GTP Signaling

To monitor GTP signaling, you can examine the messages and byte counts on Gn, S5, Gp, and S8 interfaces (statistics per APN, QCI per ARP, per GTP version, global).

You can also examine:

- Per peer history
- Per GTP cause code statistics for granular measurement of the number of failures
- Separate session establishments attempts/success counts
- Separate statistics for IPv4, IPv6, and dual address stack sessions

The following examples show how you can monitor GTP on the P-GW from the CLI.

1. To see the state of services PICs and PFEs, enter this command:

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

Client	State	Redundancy Role
pfe-0/2/0	In-Service	Primary
pfe-0/0/0	In-Service	Primary
ms-4/0/0	In-Service	Primary

2. To see the resource management filters for GTP packet steering, enter the command:

```
user@host> show unified-edge rmpps filters
```

3. To see a summary of subscribers on the gateway, enter the command:

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

4. To see subscriber details, enter the command:

```
user@host> show unified-edge ggsn-pgw subscribers extensive
```

5. To show all GTP statistics (including messages sent and received, and cause codes sent and received), enter the command:

```
user@host> show unified-edge ggsn-pgw gtp statistics detail
```

6. To see all the GTP peers, enter the command:

```
user@host> show unified-edge ggsn-pgw gtp peer detail
```

- Related Documentation**
- [Monitoring the Mobile Environment - Key Performance Indicators on page 429](#)
 - [Monitoring Resources on page 430](#)

Monitoring Session Status

Current session/ bearer counts can be monitored at various levels. For example, per APN, per QCI/ARP, global, per RAT type, per APN, or per QCI.

A useful command to show these types of statistics is:

```
user@host> show unified-edge ggsn-pgw qos statistics ?
```

Possible completions:

```
<[Enter]>      Execute this command
apn            APN name
arp           GTPv2 ARP Value (1..15)
gateway       Show subscriber for a gateway
gtpv1-arp     GTPv1 ARP Value (1..3)
qci           Show QCI statistics information (1..9)
traffic-class Show statistics for a traffic-class level
traffic-handling-priority Traffic handling priority (1..3)
|            Pipe through a command
{backup}[edit]
user@host>
```

Use this command to examine session status indicators at the APN, gateway, and other levels.

- Related Documentation**
- [Monitoring the Mobile Environment - Key Performance Indicators on page 429](#)
 - [Monitoring Resources on page 430](#)

Monitoring CPU Indicators

Monitoring CPU utilization relies on gathering data from session PICs.

To see status indicators for all PICs, enter:

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

To see status indicators for the gateway, enter:

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

```
Mobile gateway status of fpc slot: 0 pic slot: 0
```

```
State      :      Backup
Active Subscribers :      99652
Active Sessions  :      99652
Active Bearers   :      99652
CPU Load (%)    :        0
Memory Load (%) :       29
```

```
Mobile gateway status of fpc slot: 0 pic slot: 1
```

```
State      :      Active
Active Subscribers :      99652
Active Sessions  :      99652
Active Bearers   :      99652
CPU Load (%)    :        3
Memory Load (%) :       97
```

```
Mobile gateway status of fpc slot: 2 pic slot: 0
```

```
Active Subscribers :        0
Active Sessions  :        0
Active Bearers   :        0
CPU Load (%)    :        0
Memory Load (%) :       25
```

```
Mobile gateway status of fpc slot: 2 pic slot: 1
```

```
Active Subscribers :        0
Active Sessions  :        0
Active Bearers   :        0
CPU Load (%)    :        0
Memory Load (%) :       25
```

To see status indicators for an individual PIC (in the example shown, fpc-slot 2 pic-slot 0), enter:

```
user@host> show unified-edge ggsn-pgw status fpc-slot 2 pic-slot 0
```

- Related Documentation**
- [Monitoring the Mobile Environment - Key Performance Indicators on page 429](#)
 - [Monitoring Resources on page 430](#)
 - [Monitoring Memory Indicators on page 433](#)

Monitoring Memory Indicators

You can monitor system memory by gathering data from session PICs just as you do for CPU usage.

To see memory indicators for all PICs, enter:

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

To see memory indicators for an individual PIC (in the example shown, fpc-slot 2 pic-slot 0), enter:

```
user@host> show unified-edge ggsn-pgw status fpc-slot 2 pic-slot 0
```

Additionally, users with vty command privileges can check system load as well. This is an average of CPU and memory load and displays as “current system load.” This command is:

```
user@host> show mcos gw-resource tbl
```

- Related Documentation**
- [Monitoring the Mobile Environment - Key Performance Indicators on page 429](#)
 - [Monitoring Resources on page 430](#)
 - [Monitoring CPU Indicators on page 432](#)

Monitoring Charging Gateways

Charging gateways can be monitored by checking status, pending CDR counts, and per transport profile.

The specific statistics you can gather per charging gateway are:

- Status (alive or dead)
- Number of echo requests: transmitted, received, and timeouts
- Number of echo responses: transmitted and received
- Number of version unsupported packets: transmitted and received
- Number of node alive requests: transmitted and received
- Number of node alive responses: transmitted and received
- Number of redirection requests: received
- Number of redirection responses: transmitted
- Number of data record transfer requests: transmitted and timeouts

- Number of data record transfer success responses: received
- Total round trip time of previous DRT (avg, max, min)

The following commands are examples of charging gateway statistics:

```
user@host> show unified-edge ggsn-pgw charging path stat
Charging Path Status Peer-Addr Peer-Name Local-Address Status Echo
1.1.1.1 cg1 10.10.10.10 Down Enabled
```

```
Charging Path Status
Peer-Addr Peer-Name Local-Address Status Echo
1.1.1.1 cg1 10.10.10.10 Down Enabled
```

```
user@host> show unified-edge ggsn-pgw charging path statistics
```

```
Charging Path Statistics

CGF Address      : 1.1.1.1    CGF Server Name   : cg1
Echo Requests    Rx: 0      Echo Responses    Tx: 0
Echo Responses   Rx: 0      Echo Requests     Tx: 6711
Node-Alive Requests Rx: 0    Node-Alive Responses Tx: 0
Version Not Supported Rx: 0   Version Not Supported Tx: 0
Echo Requests timed out : 6710 Echo Interval      : 70
Down Detection Interval : 10   Reconnect Time Interval : 10
Destination Port      : 3386   Pending Queue Size  : 0
Path Manager FPC Slot  : 1     Path Manager PIC Slot : 0
T3 Response Time Interval : 5   Path Manager Port    : 30241
Source Interface Valid : Yes    GTPP Header Type     : long
N3 Requests          : 3       Local Address        : 10.10.10.10
GTPP Version          : V0     Transport Protocol    : UDP
```

```
user@host> show unified-edge ggsn-pgw charging transfer status
```

```
Charging Transfer Status
Transport-Profile : tp1
Total UnAck CDR's : 0
Total Buffered CDR's : 0
```

```
user@host> show unified-edge ggsn-pgw charging path statistics
```

```
Charging Path Statistics

CGF Address      : 1.1.1.1    CGF Server Name   : cg1
Echo Requests    Rx: 0      Echo Responses    Tx: 0
Echo Responses   Rx: 0      Echo Requests     Tx: 6711
Node-Alive Requests Rx: 0    Node-Alive Responses Tx: 0
Version Not Supported Rx: 0   Version Not Supported Tx: 0
Echo Requests timed out : 6710 Echo Interval      : 70
Down Detection Interval : 10   Reconnect Time Interval : 10
Destination Port      : 3386   Pending Queue Size  : 0
Path Manager FPC Slot  : 1     Path Manager PIC Slot : 0
T3 Response Time Interval : 5   Path Manager Port    : 30241
Source Interface Valid : Yes    GTPP Header Type     : long
```


N3 Requests	: 3	Local Address	: 10.10.10.10
GTPP Version	: V0	Transport Protocol	: UDP

- Related Documentation**
- [Monitoring the Mobile Environment - Key Performance Indicators on page 429](#)
 - [Monitoring Resources on page 430](#)

Monitoring Data Path Measurements

Data path measurements include:

- Data path Gn statistics, including the number of incoming/outgoing GTP data packets/octets on the Gn interface
- Number of discarded GTP data packets
- Data path charging statistics, including per rating-group (bearer) up and down packets/bytes
- Data path Gi/IP measurements (does not include drops on the Gi Packet Forwarding Engine)
- Incoming and outgoing packets/octets on the Gi interface
- Discarded packets
- Data path debug and miscellaneous statistics (includes number of in-progress sessions, deleting sessions, source address violations, per APN ACL violations, and so on).
- Accurate per subscriber packet/byte statistics
- Per Traffic Class packet and byte counts statistics (also per APN, global)
- IP measurements

- Related Documentation**
- [Monitoring the Mobile Environment - Key Performance Indicators on page 429](#)
 - [Monitoring Resources on page 430](#)

Monitoring Call Rate Statistics

The following metrics are available in real time to monitor performance of the gateway call-rate indicators:

- Real-time measure of number of calls set up in the previous configurable interval
- Real-time measurement of session deactivations displayed per configurable interval
- Total data packets processed by the gateway in the past configured interval
- Total bytes of traffic handled by the gateway in the past interval

Monitoring Data Rate Statistics

To monitor data rate statistics, enter:

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

Control plane statistics:

```
Session establishment attempts:    1
Successful session establishments:  1
MS/peer initiated session deactivations: 2
Successful MS/peer initiated deactivations: 2
Gateway initiated session deactivations: 0
Successful gateway initiated deactivations: 0
```

Data plane GTP statistics (Gn/S5/S8):

```
Input  packets:    0
Input  bytes:      0
Output packets:    7751
Output bytes:     7251652
Discarded packets: 0
```

Data plane GTP statistics (Gi):

```
Input  packets:    7751
Input  bytes:     7251652
Output packets:    0
Output  bytes:      0
Discarded packets: 0
```

The following commands can be used for data plane statistics. There are two sets of statistics (one for the Gn interface and another for the Gi interface). The commands can be used either at the APN or the gateway level.

1. To see the gateway data plane statistics, use this command:

```
user@host> show unified-edge ggsn-pgw statistics gateway gateway-name
```

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:    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
```

2. To see the APN data plane statistics, use this command:

```
user@host> show unified-edge ggsn-pgw apn statistics apn-name apn-name
```

Control plane APN 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
MS initiated modification attempts: 0
Successful MS initiated modifications: 0
PGW/GGSN initiated modification attempts: 0
Successful PGW/GGSN initiated modifications: 0
User authentication statistics:
  Authentication failures: 0
  Attempted authentications: 0
  Successful authentications: 0
Address allocation statistics:
  dynamic IP allocation attempts: 0
  dynamic IP allocation success: 0
Charging statistics:
  Number of CDRs allocated: 0
  Number of partial CDRs allocated: 0
  Number of CDRs closed: 0
  Number of containers closed: 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
Miscellaneous Packet statistics:
  IPv6 Router Solicitations received: 0
  IPv6 Router 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

```

- Related Documentation**
- [Monitoring the Mobile Environment - Key Performance Indicators on page 429](#)
 - [Monitoring Resources on page 430](#)

Tracing Control Packets

- [Requirements on page 438](#)
- [Tracing Control Packets on page 438](#)
- [Configuration on page 442](#)

Requirements

This example uses the following hardware and software components:

- An operational MX chassis
- Junos OS Mobility package

Tracing Control Packets

This section shows how to trace Gi to Gn control packets.

To efficiently monitor the data path, perform the following checks:

- Verify that the Gn interface (IFL) is receiving packets.

```
user@host> show jnh if statistics
```

IFL Name	Index	In(Packets/Bytes)	Out(Packets/Bytes)

Verify that the packets are hitting the filter.

```
user@host> show filter
```

Program Filters:

Index	Dir	Cnt	Text	Bss Name

Term Filters:

Index	Semantic	Name

1	Classic	__default_bpdu_filter__
17000	Classic	__default_arp_policer__
57008	Classic	__cfm_filter_shared_lc__
65280	Classic	__auto_policer_template__
65281	Classic	__auto_policer_template_1__
65282	Classic	__auto_policer_template_2__
65283	Classic	__auto_policer_template_3__
65284	Classic	__auto_policer_template_4__
65285	Classic	__auto_policer_template_5__
65286	Classic	__auto_policer_template_6__
65287	Classic	__auto_policer_template_7__
65288	Classic	__auto_policer_template_8__
46137345	Classic	HOSTBOUND_IPv4_FILTER

```
46137346 Classic HOSTBOUND_IPv6_FILTER
67108864 Classic __mobile_gw_impl_filter__ <<<<<<<<<<
```

Display counters for index 67108864.

```
user@host> show filter index 67108864 counters
```

Filter Counters/Policers:

Index	Packets	Bytes	Name
67108864	5	1025	__gtpc_pkt_count
67108864	5	500	__gtpu_pkt_count
67108864	0	0	__mgw_ip_frags_count
67108864	0	0	__sp-1-0_GTP_pkt_count
67108864	0	0	__sp-1-0_LIBAAA_pkt_count
67108864	0	0	__sp-1-0_LIBCHRG_pkt_count

Check the group TEID route table.

```
user@host> show route gtp-c
```

1/8	Service 653
1.0/13	Service 653
1.0.0.0/40	Service 653



NOTE: The 1 at the beginning here is the GTP-C route-type. If the *teid=0* route (1.0.0.0/40) is missing, verify that *rmrpsd* on the Routing Engine installed those routes or verify that it is running.

```
user@host> show filter nexthops
```

Name	Protocol	Type	Option	Refcount	NH ID
ms-1/0/0.16000:mgw:SPFE-AAA	IPv4	service	0x01	0	650
ms-1/0/0.16000:mgw:SPFE-CHRG	IPv4	service	0x01	0	648
ms-1/0/0.16000:mgw:SPFE-SMA	GTP-U	service	0x01	0	653
ms-1/0/0.16000:mgw:SPFE-UPIC	GTP-U	service	0x01	0	656

Display details on service 653.

```
user@host> show nhdb id 653 extensive
```

ID	Type	Interface	Next Hop Addr	Protocol	Encap	MTU	Flags	PFE internal
653	Service	-	-	GTP-U	-	0	0x00000000	0x00000000

Target NH: 654
PFE#0, Target Addr = 0x1fcbcl
SvcDesc = 0x1fcbff
PFE#1, Target Addr = 0x1fcbfe
SvcDesc = 0x1fcbfd

Verify the nexthop target 654.

```
user@host> show nhdb id 654 extensive
```

ID	Type	Interface	Next Hop Addr	Protocol	Encap	MTU	Flags	PFE internal
Flags								

Check whether the NH-id point to the correct ms-ifl.

```
user@host> show mobile-edge halp ucode-nhs
```

Nexthop ID	Purpose
4194306	GTPv0 parsing ucode
4194307	GTP-C v1/v2 parsing ucode
4194308	GTP-U swap ports ucode
4194309	DHCP parsing ucode
4194310	GTP-C table NH
4194311	GTP-U table NH

Check to see whether packets are discarded or punted the to host.

```
user@host> show jnh 0 exceptions
```

Ucode Internal ----- mcast stack overflow

...

Packet Exceptions

bad ipv4 hdr checksum	DISC(2)		
non-IPv4 layer3 tunnel	DISC(4)	0	0
GRE unsupported flags	DISC(5)	0	0
tunnel pkt too short	DISC(6)	0	0
bad IPv6 options pkt	DISC(9)	0	0
bad IP hdr	DISC(11)	0	0
bad IP pkt len	DISC(12)	0	0
L4 len too short	DISC(13)	0	0
invalid TCP fragment	DISC(14)	0	0
mtu exceeded	DISC(21)	0	0
frag needed but DF set	DISC(22)	0	0
ttl expired	PUNT(1)	0	0
IP options	PUNT(2)	0	0
control pkt punt via ucode	PUNT(4)	0	0
frame format error	DISC(0)		
tunnel hdr needs reassembly	PUNT(8)	0	0
GRE key mismatch	DISC(76)	0	0
my-mac check failed	DISC(28)		
frame relay type unsupported	DISC(38)	0	0
IGMP snooping control packet	PUNT(12)	0	0
bad CLNP hdr	DISC(43)	0	0
bad CLNP hdr checksum	DISC(44)	0	0
incorrect length in GTP header	DISC(45)	0	0
GTP header errors	DISC(46)	0	0
Bearer using different IP address	DISC(47)	0	0
expecting sequence number	DISC(48)	0	0

```
sequence number isnt correct    DISC(49)    0    0
SR is marked for traffic discard DISC(50)    0    0
```

Firewall

```
-----
mac firewall          DISC(78)
firewall discard      DISC(67)    0    0
tcam miss             DISC(16)    0    0
firewall reject       PUNT(36)    0    0
firewall send to host PUNT(53)    0    0
```

Routing

```
-----
discard route         DISC(66)    0    0
hold route            DISC(70)    0    0
mcast rpf mismatch    DISC( 8)    0    0
resolve route         PUNT(33)    0    0
control pkt punt via nh PUNT(34)    0    0
host route            PUNT(32)  2313  92940
ICMP redirect         PUNT( 3)    0    0
mcast host copy       PUNT( 6)    0    0
reject route          PUNT(40)    0    0
```

Misc

```
-----
debug                 DISC(65)    0    0
services pkt internal test PUNT(38)    0    0
directed bcast        DISC(89)    0    0
virtual-chassis pkt(hi) PUNT(54)    0    0
virtual-chassis pkt(lo) PUNT(55)    0    0
virtual-chassis error   DISC(42)    0    0
ME-subscriber policing out of spec packet dropsDISC(52)    0    0
```

To display non-zero counters, enter:

```
host@user> show jnh 0 exceptions terse
```

```
Reason          Type    Packets  Bytes
=====
```

Routing

```
-----
host route      PUNT(32)  2393  96140
```

Another example is: a v2 call comes in with QCI 5 and gets mapped to FC af5. On that queue, you can see the PPS for the Gn-facing interface and the Gi-facing interface

```
user@host> show interfaces queue ge-1/2/5 forwarding-class af5
```

Where 1/2/5 is the Gn-facing interface. Then enter:

```
user@host> show interfaces queue ge-1/2/1 forwarding-class af5
```

Where 1/2/1 is the Gi-facing interface.

Configuration

- [Tracing Packets on page 442](#)

Tracing Packets

Results This example illustrated the steps you can take to trace control packets.

- Related Documentation**
- [Monitoring the Mobile Environment - Key Performance Indicators on page 429](#)
 - [Monitoring Resources on page 430](#)

How to Trace Data Packets from Gn to Gi Interfaces

- [Requirements on page 442](#)
- [Tracing Data Packets on page 442](#)
- [Configuration on page 442](#)

Requirements

This example uses the following hardware and software components:

- An operational MX chassis
- Junos OS Mobility package

Tracing Data Packets

This section shows how to trace Gn to Gi (GTP-U) data packets.

Configuration

- [Setting up Data Packet Tracing on page 442](#)

Setting up Data Packet Tracing

Step-by-Step Procedure The following procedure shows how to trace GTP-U (Gn to Gi) data packets.

1. Verify that the Gn/S5 interface is receiving packets.

```
user@host> show jnh if statistics
```

IFL Name	Index	In(Packets/Bytes)	Out(Packets/Bytes)
...			

2. Verify that the filter is seeing GTP-U packets by finding the index of the implicit RTT filter used by mobility applications.

```
user@host> show filter UE address prefix
```

```
Program Filters:
```

```
-----
```


Index	Dir	Cnt	Text	Bss	Name

Term Filters:

Index	Semantic	Name

2	Classic	__default_bpdu_filter__
17000	Classic	__default_arp_policer__
57008	Classic	__cfm_filter_shared_lc__
65280	Classic	__auto_policer_template__
65281	Classic	__auto_policer_template_1__
65282	Classic	__auto_policer_template_2__
65283	Classic	__auto_policer_template_3__
65284	Classic	__auto_policer_template_4__
65285	Classic	__auto_policer_template_5__
65286	Classic	__auto_policer_template_6__
65287	Classic	__auto_policer_template_7__
65288	Classic	__auto_policer_template_8__
46137345	Classic	HOSTBOUND_IPv4_FILTER
46137346	Classic	HOSTBOUND_IPv6_FILTER
46137347	Classic	__me_uplink_exception_filter_ipv4__
46137349	Classic	__me_uplink_exception_filter_ipv6__
67108864	Classic	__mobile_gw_impl_filter__ <----

3. Verify that the filter has the correct GGSN IP address (172.23.9.100 in the following output) in the filter.

```
user@host> show filter index 67108864 program
```

```
Filter index = 67108864
Optimization flag: 0xf7
Filter notify host id = 0
Filter properties: None
Filter state = CONSISTENT
term IP-Fragments
term priority 0
  is-fragment
    value & 0x3fff != 0x0000
    false branch to match protocol in rule GTP-U
  destination-address
    172.23.9.100/32 <----
    false branch to match protocol in rule GTP-U

  then
    action next-hop, type (nh-id)
      4194308
    count __mgw_ip_frgs_count
term GTP-U
term priority 0
  protocol
    17
    false branch to match action in rule default-term
  port
    2152
    false branch to match port in rule GTP-C
```

```

destination-address
  172.23.9.100/32 <----
  false branch to match port in rule GTP-C

then
  action next-hop, type (nh-id)
    4194308
  count __gtpu_pkt_count
term GTP-C--
term priority 0
port
  2123
  false branch to match port in rule sp-1/0_LIBAAA_udp_start_10000
destination-address
  172.23.9.100/32
  false branch to match port in rule sp-1/0_LIBAAA_udp_start_10000

then
  action next-hop, type (nh-id)
    4194307
  count __gtpc_pkt_count

```

4. Verify that the implicit RTT firewall filter counter for GTP-U is incrementing.

```
user@host> show filter index 67108864 counters
```

Filter Counters/Policers:

Index	Packets	Bytes	Name
67108864	2	452	__gtpc_pkt_count
67108864	2	584	__gtpu_pkt_count <----
67108864	0	0	__mgw_ip_frgs_count
67108864	0	0	__sp-1-0_GTP_pkt_count
67108864	0	0	__sp-1-0_LIBAAA_pkt_count
67108864	0	0	__sp-1-0_LIBCHRG_pkt_count

5. Verify that the GTP-U ingress ucode NH is created and is not marked as *Discard*.

```
user@host> show mobile-edge halp ucode-nhs
```

Nexthop ID	Purpose
4194306	GTPv0 parsing ucode
4194307	GTP-C v1/v2 parsing ucode
4194308	GTP-U ingress ucode
4194309	DHCP parsing ucode
4194310	GTP-C table NH
4194311	GTP-U table NH
4194312	GTP-U restore packet context ucode
4194313	IP frag load balancing ucode

```
host@user> show nhdb id 4194308 extensive
```

ID	Type	Interface	Next Hop Addr	Protocol	Encap	MTU	Flags	PFE internal
4194308	Unicast	-	-	GTP-U	-	0	0x00000000	0x00008004

```
Flags:      0x00000000
PFE internal flags: 0x00008004
```

```
Dram Bytes   : 268
PreComputed MTU: 0
Flags        : 0x0
Parent NHID   : 0
```

```
PFE:0
```

```
Encap-ptr chain:
-----
```

```
Dram Bytes: 268
```

6. Verify that the GTP-U route table is set up correctly on the Gn ingress Packet Forwarding Engine.

```
host@user> show route gtp-u
```

```
default          Service 653
0.0.0.0          Service 647
0.32/16          Unicast 666 mif.16000
```



NOTE: Data TEID route should be present in the gtp-u table (0.32/16 in this case, which is teid starting with 0x02). Since any Packet Forwarding Engine can be ingress Packet Forwarding Engine, the same GTP-U route table is present on all Packet Forwarding Engines. NH-id 666 in the route corresponds to the anchor Packet Forwarding Engine.

7. To find the anchor Packet Forwarding Engine, execute the following command. The L2 interface identifies the anchor Packet Forwarding Engine. In the output below, fpc 0 pic 0 is the anchor Packet Forwarding Engine.

```
host@user> show nhdb id 666 extensive
```

```
ID Type Interface Next Hop Addr Protocol Encap MTU Flags PFE internal
Flags
666 Unicast mif.16000 default IPv4 Unspecified 0 0x10000000
0x00000000
```

```
Flags:      0x10000000
PFE internal flags: 0x00000000
L2-Interface: pfe-0/0/0.16383 (81) <----- ANCHOR PFE
```

```
Dram Bytes   : 268
PreComputed MTU: 0
Flags        : 0x10000000
Parent NHID   : 0
Feature List: NH
[pfe-0]: 0xce811db000200005;
```

```
f_mask:0x00400000; c_mask:0x80000000; f_num:11; c_num:1, inst:0
Idx#9   ucast:
[pfe-0]: 0xce811db000200005
```

```
<.....SNIP.....>
```

8. Verify that the subscriber is installed in the anchor Packet Forwarding Engine (LU id = 0 here).

```
host@user> show vbf hw 0 subscriber-table uplink
```

```
+-----+-----+-----+-----+-----+-----+-----+-----+
| RINDEX | TEID  | VRF ID | TFT ID | CONFIG | FLAGS | CHRGID | CHRGADDR |
| IPADDR |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 0xf    | 0x200001 | 0x0    | 0x0    | 0x2210 | 0x1    | 0x0    | 0x80000e | 0x27270802 |
| 0xb    | 0x200000 | 0x0    | 0x0    | 0x2210 | 0x1    | 0x0    | 0x800000 | 0x27270801 |
+-----+-----+-----+-----+-----+-----+-----+-----+
| TOTAL: 2                                     |
+-----+-----+-----+-----+-----+-----+-----+-----+
```

9. Verify that there are no GTP parsing errors on the anchor Packet Forwarding Engine.



NOTE: Also verify that the *ln* stats on the Gn (S5) interface are incrementing.

```
st@user> show vjnh 0 exceptions terse
```

- Related Documentation**
- [Monitoring the Mobile Environment - Key Performance Indicators on page 429](#)
 - [Monitoring Resources on page 430](#)

Trace Data Packets from Gi to Gn Interfaces

- [Requirements on page 446](#)
- [Tracing Data Packets on page 446](#)
- [Configuration on page 447](#)

Requirements

This example uses the following hardware and software components:

- An operational MX chassis
- Junos OS Mobility package

Tracing Data Packets

This topic shows how to trace Gi to Gn data packets.

Configuration

- [Setting up Data Packet Tracing on page 447](#)

Setting up Data Packet Tracing

Step-by-Step Procedure

The following examples explain how to trace Gi to Gn data packets.

1. Verify that an aggregate route is installed. In this case, aggregate route 39.39.4/22 for user equipment is present in the Gi VRF (inet.0 in the following example).

```
user@host> show mobile-gateways subscribers
```

MSISDN	Subscriber Address	Peer Address	APN
1234567890	39.39.4.1	172.23.9.196	internet123
1234567891	39.39.4.2	172.23.9.196	internet123

2. To see details for subscribers, enter:

```
user@host> show mobile-gateways subscribers extensive
```

```
MSISDN : 1234567890      Subscriber Address - V4 : 39.39.4.1
IMSI : 22321321312336f  Control Plane Peer Address : 172.23.9.196
NSAPI/EBI : 5           Data Plane Peer Address : 172.23.9.196
Control TEID - Local : 8000000 Remote : 101
Data TEID - Local : 100000 Remote : 102
APN name : internet123   Charging ID : 8000000
Control - FPC : 1 PIC : 0 Anchor PFE : 129
QCI/ARP : 5 /0   GBR : 0   MBR : 0
Subscriber state : Established Bearer State : Established
Bearer Substate : -
Last statistics collection time : None collected
```

```
MSISDN : 1234567892      Subscriber Address - V4 : 39.39.4.2
IMSI : 22321321312337f  Control Plane Peer Address : 172.23.9.196
NSAPI/EBI : 5           Data Plane Peer Address : 172.23.9.196
Control TEID - Local : 8000001 Remote : 103
Data TEID - Local : 100001 Remote : 104
APN name : internet123   Charging ID : 8000001
Control - FPC : 1 PIC : 0 Anchor PFE : 129
QCI/ARP : 5 /0   GBR : 0   MBR : 0
Subscriber state : Established Bearer State : Established
Bearer Substate : -
Last statistics collection time : None collected
```

3. Since the user equipment IP address starts with **39.39**, look for aggregation routes with that prefix.

```
user@host> show route ip table index 0r
```

```
IPv4 Route Table 0, default.0, 0x0:
Destination NH IP Addr Type NH ID Interface
-----
default Reject 42
0.0.0.0 Discard 40
10.255.15.135 10.255.15.135 Local 576
```

```

12.9.1.1          12.9.1.1    Local  645 ms-1/0/0.0
29.29.29/24              Discard  626 mif.0
29.29.29.100         29.29.29.100 Local  625
39.39.4/22              Unicast  677 mif.0 <---

```

4. Verify that the NH for the aggregate route uses mif ifl for the APN to which the subscriber belongs and that the NH's L2 interface corresponds to the anchor Packet Forwarding Engine.

```
user@host> show nhdb id 677 extensive
```

```

  ID  Type  Interface  Next Hop Addr  Protocol  Encap  MTU  Flags PFE
internal Flags
-----
677  Unicast mif.0    default        IPv4  Unspecified  0  0x08000000
0x00000000

Flags:      0x08000000
PFE internal flags: 0x00000000
L2-Interface: pfe-0/0/0.16383 (82) <--- ANCHOR PFE

```

5. Verify that the anchor Packet Forwarding Engine has the subscriber entry (in this example: LU id 0).

```
user@host> show vbf hw 0 subscriber-table downlink
```

```

+-----+-----+-----+-----+-----+-----+-----+-----+
| RINDEX | VRF ID | IPADDR | CONFIG | FLAGS | CHRGID | CHRGADDR | TEID |
| NHID |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 0x4    | 0x0    | 0x27270401 | 0x2210 | 0x0    | 0x0    | 0x8000000 | 0x65 | 0x2ac |
| 0x3    | 0x0    | 0x27270402 | 0x2210 | 0x0    | 0x0    | 0x800000e | 0x67 | 0x2ac |
+-----+-----+-----+-----+-----+-----+-----+-----+
| TOTAL: 2 |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

For a specific subscriber, you can verify that it uses the right peer NH.

```
user@host> show vbf hw 0 subscriber downlink id 39.39.4.1
```

```

Key:
Major Version: 0
Minor Version: 2
Overflow: 0
TFT Rule Id: 0
Unique Id: 0
IPv4 ADDR: 0x27270401
Ext Data:
IDLE-TO PROFILE-ID: 0
AAA PROFILE-ID: 0
QCI: 5
Policing: Disabled
Reporting Stats: Disabled
Charging Stats: Enabled
Drop: 0
Send to Upic: 0
Valid: 1

```

Proto: V4
Seq Num Proc: Disabled
Gtp Ver: 1
Num VBF ext words: 0
Num VBF words: 1
Charg Stat Addr: 0x800000
Charg Profile Id: 0
Trigger Pending: 0
Vol Limit Hit: 0
Time Limit Hit: 0
Tariff Change Hit: 0
Delete Event: 0
Signal Event: 0
Tariff Id: 0
Update First: 0
Time Limit Check: 0
Chrg Inst Id: 0
Policer Type: 0
Policer Color: 0
Policer Oper: 0
Policer Count: 0
Policer Addr Offset: 0x0000
Reporting Stats Addr: 0x000000
Remote Index: 0x0006
VBF Info[0]: 0x58
VBF Info[1]: 0x17
VBF Info[2]: 0x81
VBF Info[3]: 0xaa
VBF Info[4]: 0x0
VBF Info[5]: 0x0
VBF Info[6]: 0x0
VBF Info[7]: 0x0
VBF Info[8]: 0x0
VBF Info[9]: 0x0
VBF Info[10]: 0x0
VBF Info[11]: 0x0
VBF Info[12]: 0x0
VBF Info[13]: 0x0
VBF Info[14]: 0x0
VBF Info[15]: 0x0
VBF Info[16]: 0x0
VBF Info[17]: 0x0
VBF Info[18]: 0x0
VBF Info[19]: 0x0
VBF Info[20]: 0x0
VBF Info[21]: 0x0
VBF Info[22]: 0x0
VBF Info[23]: 0x0
VBF Info[24]: 0x0
VBF Info[25]: 0x0
VBF Info[26]: 0x0
VBF Info[27]: 0x0
Sideband:
template nh vaddr: 0xd0239f
peer nh id: 0x02ac
udp src port: 0x0000000000000000

TEID: 0x000000000000065
exp seq num: 0x000000000000000



NOTE: Peer nh id 0x02ac (684 decimal) is the NH that performs the GTP encapsulation. Template NH is the MIF OIF start. Having Zero peer nh id causes the downlink traffic to fail.

6. Verify the S-GW/SGSN IP address and other fields used in the GTP encapsulation from the peer NH.

user@#host> show nhdb id 684 extensive1

ID	Type	Interface	Next Hop Addr	Protocol	Encap	MTU	Flags	PFE
684	Unicast	mif:16000	default	IPv4	Unspecified	0	0x04000000	0x00000000

Flags: 0x04000000
PFE internal flags: 0x00000000

Dram Bytes : 268
PreComputed MTU: 0
Flags : 0x4000000
Parent NHID : 0

Feature List: NH
[pfe-0]: 0x08fe5b2000010000;
[pfe-1]: 0x08fe5b1000010000;
f_mask:0x00600000; c_mask:0xc0000000; f_num:11; c_num:2; inst:-1
Idx#9 ucast:
[pfe-0]: 0x1007f2fe00ffffff
[pfe-1]: 0x1007f2f3c0ffffff

Idx#10 ifl-output:
[pfe-0]: 0x27ffff80001040c
[pfe-1]: 0x27ffff80001040c

PFE:0

Encap-ptr chain:

Encapsulation Pointer (0x46a86d58) data:
Encap-ptr-type:gtp
Ucode EType:tunnel-encaps
Ref Count:1
Control-Word: GTP(0x03)
Jnh-mem: size: 2; addr: 0x82
Key: 0x0d000003ffffff-ac1709c4ac170964401100:

GTP Details:


```

Allow Frag,

SrcIP: 172.23.9.100 <-- GGSN/MBG1 IP address

DstIP: 172.23.9.196 <-- SGSN/SGW IP address

ttl: 64
l4_proto: 17
l3_proto: V4
JNH words: 0x2802200000030000 JNH words: 0xac170964ac1709c4

```

PFE:1

Encap-ptr chain:

Encapsulation Pointer (0x46a86d58) data:

```

Encap-ptr-type: gtp
Ucode EType: tunnel-encaps
Ref Count: 1
Control-Word: GTP(0x03)
Jnh-mem: size: 2; addr: 0x84
Key: 0x0d000003ffffff-ac1709c4ac170964401100:

```

GTP Details:

Allow Frag,

SrcIP: 172.23.9.100

DstIP: 172.23.9.196

```

ttl: 64
l4_proto: 17
l3_proto: V4
JNH words: 0x2802200000030000 JNH words: 0xac170964ac1709c4

```

7. Verify that the MIF OIF features are correct.

```
user@#host> show jnh 0 vread 0xd0239f
```

```
Addr: 0xd0239f, Data = 0x08fe580000030000
```

```
NPC0(curve vty)# sh jnh 0 decode 0x08fe580000030000
```

```
CallNH: desc_ptr: 0x1fcb00, mode=0, rst_stk=0x0, count=0x3
```

```
0x1fcafc 0: 0x27ffff80001640c <-- Per subscriber Fixed classifier applied on MIF IFL
```

```
0x1fcafd 1: 0x02000fe52e000804 <-- Proto-type demux
```

```
0x1fcafe 2: 0x08fe50e000010000 <-- Mobile edge features (per subscriber policer, charging)
```

```
0x1fcaff 3: 0x1274040ea00003c0 <-- WAN out
```

8. Verify subscriber-fixed classifier applied on MIF IFL.

```
user@#host> show jnh 0 decode 0x27ffff80001640cf
```

```
UcodeNH: Vbf Indirect, var-id = VBF_VAR_IFL_FIXED_CLASSIFIER(11)
```

9. Verify the demux prototype.

```
user@#host> show jnh 0 decode 0x02000fe52e000804
IndexNH:key_ptr:0x80/0, desc_ptr=0x1fca5c, max=8, nbits=4
```

10. Verify mobile edge features (per subscriber policer, charging).

```
user@#host> show jnh 0 decode 0x08fe50e000010000

CallNH:desc_ptr:0x1fca1c, mode=0, rst_stk=0x0, count=0x1
0x1fca1a 0 : 0xc8000000725200041
0x1fca1b 1 : 0xc8000000000000040
```

```
NPC0(curve vty)# sh jnh 0 decode 0xc8000000725200041
```

```
JNH_ME_NH:
opcode = 0x00000019
desc_ptr = 0x00000000
data = 0x39290002
func_code = 0x00000001
JNH_ME_NHDATA_ME_POLICER:
normal = 0x0000e4a4
ext_data = 0x00000000
default = 0x00000000
parameterized = 0x00000001
next_nh = 0x00000000
```

```
NPC0(curve vty)# sh jnh 0 decode 0xc8000000000000040
```

```
JNH_ME_NH:
opcode = 0x00000019
desc_ptr = 0x00000000
data = 0x00000002
func_code = 0x00000000
JNH_ME_NHDATA_ME_CHARGING:
report_stat_en = 0x00000000
default = 0x00000000
parameterized = 0x00000001
next_nh = 0x00000000
```

11. Verify WAN.

```
user@#host> show jnh 0 decode 0x1274040ea00003c0
```

```
ModifyNH: Subcode=SetQueue(9),Desc=0xd0103a,Data=0x3c0,NextNH=1
```

```
Dram Bytes: 440
```

Related Documentation

- [Monitoring the Mobile Environment - Key Performance Indicators on page 429](#)
- [Monitoring Resources on page 430](#)
- [How to Trace Data Packets from Gn to Gi Interfaces on page 442](#)

How to Verify Charging Statistics Processing

- [Requirements on page 453](#)
- [Verifying Packet Forwarding Engine Charging Statistics Are Processing Properly on page 453](#)
- [Configuration on page 453](#)

Requirements

This example uses the following hardware and software components:

- An operational MX chassis
- Junos OS Mobility package

Verifying Packet Forwarding Engine Charging Statistics Are Processing Properly

This section shows an example of verifying that Packet Forwarding Engine charging statistics are processed from the LU to the Stats agent.

Configuration

- [Processing Packet Forwarding Engine Charging Statistics on page 454](#)

Processing Packet Forwarding Engine Charging Statistics

Step-by-Step Procedure The following procedure shows how to verify that charging statistics are transferred from the LU to Stats agent via TOE. The three components required to ship charging statistics from the forwarding plane to the control plane are:

- Callout thread: This is a 0.5 sec periodic thread that runs in the LU and is responsible for preparing the charging statistics.
- Charging thread: This thread runs on the LU TOE and is responsible for shipping charging statistics from the LU to the Stats agent.
- Stats agent: This runs on the Packet Forwarding Engine host CPU and is responsible for forwarding charging statistics to the charging module.

The sequence of charging statistics transfer is:

- Callout thread populates charging statistics data in the Callout FIFO.
- Callout thread triggers Charging thread to notify it of availability of data in the Callout FIFO.
- Charging thread checks whether space is available on the Stats FIFO to successfully transfer statistics from the Callout FIFO.
- If there is not enough space available on the Stats FIFO, the Charging thread aborts the statistics read from the Callout FIFO.
- If enough space is available in the Stats FIFO, then the Charging thread completes the transfer in two steps:
 - Copy statistics data from Callout FIFO to TOE Lmem.
 - DMA statistics data from TOE Lmem to Stats FIFO

Follow these steps to verify proper charging statistics handling.

1. Verify that the Callout thread is populating charging statistics in the Callout FIFO. Check the Callout FIFO descriptor to see whether the Tail (write) pointer moves. The Callout thread increments this Tail (write) pointer by the number of words that it wrote to the Callout FIFO. Therefore, if the Tail (wr) pointer moves, it means that the Callout thread is writing to the Callout FIFO.

```
user@host> show jnh 0 ucode-vars
```

```
...
ME CHRG information:
Base address           : 0xc0000026
ME CHRG fifo tail(wr)/head(rd) : 2/0  <===== Check if tail(wr)
pointer moves
ME CHRG fifo base/size   : 0x01300000/1048576
ME CHRG next walk cookie : 16140901064495857675
ME CHRG time stamp      : 335007768900
```



NOTE: In the preceding snippet, 2/0 means that Tail (write) is 2 and Head (read) is 0. A value of 2 for Tail (write) means that the Callout thread has written two words to Callout FIFO.

2. Verify that the charging thread is being triggered by the callout thread to indicate data availability for transfer. The callout thread triggers the charging thread to notify it of availability of data in the callout FIFO. To verify that the charging thread is seeing these triggers, you could dump the TOE mobile-edge counters where the count of triggers from the callout thread is maintained. The count represents the count of triggers that the charging thread is able to honor—that is, the charging thread has determined that there are enough resources available to initiate a transfer.

```
user@host> show toe pfe 3 lu 0 mobile-edge counters
```

Counter block location in LMEM: 0x4270

```
Host FIFO full      : 0
Callout FIFO empty  : 0
Host addr buff size unaligned : 0
Host addr page size unaligned : 53
Test Reg 1          : 0
Test Reg 2          : 0
Callout-to-LMEM copy bytes : 231368
LMEM-to-Host dma bytes  : 231368
Callout triggers    : 2675      <=== count of triggers from Callout thread
```

3. Verify that the Stats FIFO is full. The charging thread checks whether space is available on the Stats FIFO to successfully transfer statistics from the callout FIFO. If the Stats FIFO is full, the transfer is not initiated. For each trigger from the callout thread, the charging thread checks the status of the Stats FIFO and if it is full, increments the counter.

```
user@host> show toe pfe 3 lu 0 mobile-edge counters
```

Counter block location in LMEM: 0x4270

```
Host FIFO full      : 0      <=== increments on each trigger from
                               Callout thread, if Stats FIFO is FULL and
                               trigger cannot be "honored"
Callout FIFO empty  : 0
Host addr buff size unaligned : 0
Host addr page size unaligned : 53
Test Reg 1          : 0
Test Reg 2          : 0
Callout-to-LMEM copy bytes : 231368
LMEM-to-Host dma bytes  : 231368
Callout triggers    : 2675
```

4. Verify that the charging thread is reading the charging statistics from the callout FIFO. Check the TOE mobile-edge counters to get the total number of “bytes” of

charging data transferred by the Charging thread, from the Callout FIFO to the TOE LMem.

```
user@host> show toe pfe 3 lu 0 mobile-edge counters
```

```
Counter block location in LMEM: 0x4270
```

```
Host FIFO full      : 0
Callout FIFO empty  : 0
Host addr buff size unaligned : 0
Host addr page size unaligned : 53
Test Reg 1          : 0
Test Reg 2          : 0
Callout-to-LMEM copy bytes : 231368  <== Number of bytes transferred from
                                         Callout FIFO to TOE LMem
LMEM-to-Host dma bytes   : 231368
Callout triggers        : 2675
```

5. Verify that the charging thread is sending charging data to the Stats FIFO. Check the TOE mobile-edge counters to get the number of “bytes” of charging statistics transferred by the charging thread, from the TOE LMem to Stats FIFO.

```
user@host> show toe pfe 3 lu 0 mobile-edge counters
```

```
Counter block location in LMEM: 0x4270
```

```
Host FIFO full      : 0
Callout FIFO empty  : 0
Host addr buff size unaligned : 0
Host addr page size unaligned : 53
Test Reg 1          : 0
Test Reg 2          : 0
Callout-to-LMEM copy bytes : 231368
LMEM-to-Host dma bytes   : 231368  <=== Number of bytes transferred by
                                         charging thread from TOE LMem to Stats
FIFO
Callout triggers        : 2675
```

- Related Documentation**
- [Monitoring the Mobile Environment - Key Performance Indicators on page 429](#)
 - [Monitoring Resources on page 430](#)

CHAPTER 15

Troubleshooting

This chapter describes the proper actions to take to restore network health when performance or processes are not behaving as expected.

- [Troubleshooting Overload Conditions in the Mobile Network on page 457](#)
- [Troubleshooting Multilevel Overload Protection on page 457](#)
- [Responding to an Overload on page 458](#)
- [Monitoring GTP Signaling on page 458](#)
- [Troubleshooting Alarms, Logs, and Traps on page 459](#)
- [Troubleshooting Admission Control on page 461](#)
- [Monitoring AAA Metrics on page 463](#)

Troubleshooting Overload Conditions in the Mobile Network

The common causes of an overload condition are:

- An external server (RADIUS, DHCP, charging gateway, PCRF, and so on) is down for an extended period of time
- A burst of GTP control messages from a rebooted peer
- Capacity overload due to oversubscribed system limits
- Management operations such as bulk session deletes
- Peer reboot leading to bulk deletes resulting in higher CPU consumption

Related Documentation

- [Troubleshooting Mobility](#)

Troubleshooting Multilevel Overload Protection

To troubleshoot multilevel overloads, consider:

- Configurable low and high thresholds in percentage for each resource monitored
- Configurable Local policy to apply when the resource low or high threshold is reached



NOTE: For example: When memory usage reaches 70%, accept only calls with an allocation and retention priority (ARP) of 5 and higher. When memory usage reaches 90%, accept only calls with ARP of 3 or higher.

- Internal redirection policy to equally distribute calls to various session PICs in the chassis

**Related
Documentation**

- Troubleshooting Mobility
- [Responding to an Overload on page 458](#)

Responding to an Overload

To respond to an overload condition, consider:

- Apply gating to incoming calls and service high-priority subscribers
- Generate alarms, traps, and logs to notify the operator
- Throttle request generated toward external entities
- Configurable redirection policy to forward calls matching a certain criteria to an external gateway
- Configurable priority-level (ARP) to service during overload condition
- Each component dynamically reports load to the central resource controller for real-time admission control.

These are default actions that the gateway performs when overload conditions occur.

**Related
Documentation**

- Troubleshooting Mobility

Monitoring GTP Signaling

To monitor GTP signaling, you can examine the messages and byte counts on Gn, S5, Gp, and S8 interfaces (statistics per APN, QCI per ARP, per GTP version, global).

You can also examine:

- Per peer history
- Per GTP cause code statistics for granular measurement of the number of failures
- Separate session establishments attempts/success counts
- Separate statistics for IPv4, IPv6, and dual address stack sessions

The following examples show how you can monitor GTP on the P-GW from the CLI.

1. To see the state of services PICs and PFEs, enter this command:

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


Client	State	Redundancy Role
pfe-0/2/0	In-Service	Primary
pfe-0/0/0	In-Service	Primary
ms-4/0/0	In-Service	Primary

2. To see the resource management filters for GTP packet steering, enter the command:

```
user@host> show unified-edge rmpps filters
```

3. To see a summary of subscribers on the gateway, enter the command:

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

4. To see subscriber details, enter the command:

```
user@host> show unified-edge ggsn-pgw subscribers extensive
```

5. To show all GTP statistics (including messages sent and received, and cause codes sent and received), enter the command:

```
user@host> show unified-edge ggsn-pgw gtp statistics detail
```

6. To see all the GTP peers, enter the command:

```
user@host> show unified-edge ggsn-pgw gtp peer detail
```

Related Documentation

- [Monitoring the Mobile Environment - Key Performance Indicators on page 429](#)
- [Monitoring Resources on page 430](#)

Troubleshooting Alarms, Logs, and Traps

The mobility system generates and retains the following congestion statistics:

Current congestion status peak congestion hits

- Time when the last congestion occurred
- Duration the last congestion lasted
- Number of calls rejected during congestion
- SNMP traps
- System logs

The following are GTP traps:

- jnxMbgPgwGtpPeerGWUpNotif

The state of a GTP peer (control or data) has changed to UP. The GTP peer in trap is specified as "Rem: 200.6.1.2 Loc: 200.6.88.1 vrf: 0 [Ctrl]" where 'Rem' is the remote IP address, 'Loc' is the local IP address, and 'vrf' is the vrf instance. 'Ctrl' indicates that this is a GTP-C peer. For the GTP-U peer, string 'Data' is present in place of 'Ctrl'. This trap is generated only if GTP path management for the GTP peer is enabled.

- jnxMbgPgwGtpPeerDownNotif

The state of a GTP peer (control or data) has changed to DOWN. The GTP peer in trap is specified as "Rem: 200.6.1.2 Loc: 200.6.88.1 vrf: 0 [Ctrl]" where 'Rem' is the remote IP address, 'Loc' is the local IP address, and 'vrf' is the vrf instance. 'Ctrl' indicates that this is GTP-C peer. For GTP-U peer, string 'Data' will be present in place of 'Ctrl'. This trap is generated only if GTP path management for the GTP peer is enabled.

- **jnxMbgPgwGtpPeerDNThresPerPeerNotif**

The total number of GTP peer (control or data) down events per GTP peer have crossed a threshold. The GTP peer in trap is specified as "Rem: 200.6.1.2 Loc: 200.6.88.1 vrf: 0 [Ctrl]" where 'Rem' is remote IP address, 'Loc' is local IP address, 'vrf' is vrf instance. 'Ctrl' indicates that this is GTP-C peer. For GTP-U peer, string 'Data' is present in place of 'Ctrl'. If the number becomes higher than the "raise threshold," then value 1 in field jnxMbgPgwGtpAlarmState indicates the alarm-state "raised," and if the number becomes less than "clear threshold," then value 0 in field jnxMbgPgwGtpAlarmState indicates alarm-state "cleared". This trap is generated only if GTP path management for the GTP peer is enabled.

- **jnxMbgPgwGtpNumDiscardedGtpcPktThresNotif**

- The following are the Subscriber Manager traps:

- **jnxMbgPgwSMGtpEventNotif**

An important GTP event has occurred. jnxMbgPgwSMGTPEventType indicates the type of event (for example, "PDP_CTXT_CREATE_REJECT") and jnxMbgPgwSMGTPEventCause indicates the cause of the event (for example, "RESOURCE_ERR").

- **jnxMbgPgwSMSubscribersThresGblNotif** The total number of subscribers in the system has crossed a threshold.



NOTE: For this trap and all remaining Subscriber Manager traps, two thresholds ("High" and "Low") have been defined. For each threshold, this notification is generated when a threshold is crossed. The notification is not generated as soon as the threshold is crossed. The notification with jnxMbgPgwSMAlarmState = "RAISED" is generated if this notification has not already been generated for a threshold or the trap with jnxMbgPgwSMAlarmState = "CLEARED" has been generated for a threshold and the number stays above a threshold for a duration of 3 minutes (default) . The notification with jnxMbgPgwSMAlarmState = "CLEARED" is generated if the notification with jnxMbgPgwSMAlarmState = "CLEARED" has been generated for a threshold and the number stays below the threshold for a duration of 3 minutes (default). jnxMbgPgwSMAlarmThreshld indicates the threshold that was crossed. jnxMbgPgwSMAlarmState (RAISED/CLEARED) indicates if the number is more than the threshold ("RAISED") or is less than the threshold ("CLEARED").

- **jnxMbgPgwSMSubscribersThresPerSPNotif**

The total number of subscribers per services PIC has crossed a threshold.
jnxMbgPgwSMSPICName indicates the services PIC for which this trap was generated.

- jnxMbgPgwSMSessionEstFailThresPerSPNotif

The total number of session establishment failures per Service PIC has crossed a threshold. jnxMbgPgwSMSPICName indicates the services PIC for which this trap was generated.

- jnxMbgPgwSMSessionEstFailThresPerTCNotif

The total number of session establishment failures per traffic class (GTPv1) has crossed a threshold. jnxMbgPgwSMQCIName indicates the TC (Traffic Class) for which this trap was generated.

- jnxMbgPgwSMSessionEstFailThresPerQCINotif

The total number of session establishment failures per QoS class identifier (GTPv2) has crossed a threshold. jnxMbgPgwSMQCIName indicates the QCI for which this trap was generated.

- jnxMbgPgwSMBearersThresGblNotif

The total number of bearers in the system has crossed a threshold.

- jnxMbgPgwSMBearersThresPerSPNotif

The total number of bearers per services PIC has crossed a threshold.
jnxMbgPgwSMSPICName indicates the services PIC for which this trap was generated.

Related Documentation

- Troubleshooting Mobility

Troubleshooting Admission Control

This topic discusses class of service (CoS) and call admission control (CAC) serviceability.

To troubleshoot call admission control, you should understand the classifier policy profiles configured on your system. A classifier policy is the configuration that maps QCI (4G) and TC/THP (3G) to internal forwarding queues and defines packet loss priority. You can have multiple classifier policy profiles on your system. Therefore, understanding how these multiple classifiers interact with your system and with each other is key to understanding what to look for when you have problems with admission control.

To understand CoS, you must understand the CoS policy. This policy is the configuration that manages quality of service (QoS) parameters. You can have multiple CoS policies on your system.

CoS and CAC serviceability also depends on two other configurations:

- Resource threshold policy which controls your system for CAC. You can have multiple resource threshold policies configured on your system.

- The bandwidth pool, which allocates bandwidth sharing among APNs and the gateway. You can have multiple bandwidth pools configured on your system.

Finally, you need to know about local policies. A local policy is a collection of a classifier profile, a CoS policy profile, a resource threshold policy profile, and a bandwidth pool. A local policy is so termed because it is attached to the gateway or to individual APNs.

You can troubleshoot class of service and call admission control by examining:

- Total system bandwidth and per APN bandwidth can be configured with percentage allocations to each QCI/Traffic-Class.
- System ensures each QCI gets allocated system bandwidth optimally
- Maximum-bearers configuration for the gateway
- High or low threshold percentages for CPU, memory, system load, or maximum bearers with local policy to apply when a threshold is reached
- Forwarding-class or loss-priority definition per QCI or traffic class
- Local policy to cap maximum GBR, MBR, and AMBR values per APN

Use the following commands to troubleshoot this environment:

- For subscribers, use the command:
`user@host > show unified-edge ggsn-pgw subscribers extensive`
- For preemption lists (priority levels), use the command:
`user@host > show unified-edge ggsn-pgw status preemption-list detail`

To debug QoS negotiation parameters:

1. Check the session status to determine whether it is a visitor, roaming, or home session.
2. Look up the local policy being applied to the APN.
3. Match this local policy with its classifier profile, the CoS policy, and the bandwidth pool

To troubleshoot calls rejected by CAC:

1. Identify rejected calls by entering:
`user@host > show unified-edge ggsn-pgw qos statistics apn apn-name1`

Counters such as “No resources”, “Service denied”, “Authentication Fail”, “APN access denied” indicate rejected calls, but not necessarily by CAC.

2. To verify the cause for rejected calls, look in the Routing Engine stats section:

```
Active Bearers
CPU Load (%)
Memory Load (%)
```

These counters can indicate that the system is running out of resources.

3. To verify that resource exhaustion is the source of the problem, enter these commands:

```

user@host > show unified-edge rmpls table gateway-bearers
user@host > show unified-edge rmpls table apn-bearers
user@host > show unified-edge rmpls table anchor-pfe-bandwidth
user@host > show unified-edge rmpls table bandwidth-pools

```

Related Documentation

- Troubleshooting Mobility

Monitoring AAA Metrics

AAA server metrics include:

- Server Up/Down status traps
- Network element status traps
- Real-time latency and flow control statistics

RADIUS logs are useful for troubleshooting an AAA profile. The following sections show logs for create, update, delete, and dynamic requests.

Create Session requests communicate with the S-GW, the P-GW, and the RADIUS server in the following manner:

```

S-GW --> Create Session request --> P-GW --> Access Request --> RADIUS
P-GW <-- Access Accept <-- RADIUS
P-GW --> Accounting Start request --> RADIUS
S-GW <-- Create Session response <-- P-GW
P-GW <-- Accounting Start response <-- RADIUS
S-GW <-- Create Session response <-- P-GW

```

If **apn wait-accounting** is enabled (it is disabled by default), then the P-GW sends the Create Session response after receiving the Accounting Start response.

The following RADIUS logs show how these Create Session requests are processed. When there is a breakdown in AAA communications, the logs help you isolate the cause of the problem.

1. Access the RADIUS log, enable trace options, and look for Authentication and Accounting messages.

```

Jun 24 11:50:19 1001025 gtid:[26]tid: [2] jsimRadius(2) Access-Request
IP 10.10.2.11 20024 >

```

...

```

Jun 24 11:50:19 1013620 gtid:[24]tid: [0] Access-Accept

```

...

```

Jun 24 11:50:19 1022764 gtid:[25]tid: [1] jsimRadius(1)
Accounting-Request IP 10.10.2.11 20025 >

```

...

Jun 24 11:50:19 1033840 gtid:[26]tid: [2] **Accounting-Response**

Interim requests can be configured to generate accounting requests periodically or they are generated when the S-GW generates a Modify bearer Request. When a Modify bearer Request is received, communication with the S-GW, P-GW, and RADIUS server flows in the following manner:

```
S-GW --> Modify bearer request --> P-GW
P-GW --> Interim request --> RADIUS
P-GW <-- Dynamic request <-- RADIUS
P-GW <-- CoA <-- RADIUS
S-GW <-- Update bearer request <-- P-GW
S-GW --> Update bearer response --> P-GW
P-GW ---> CoA ACK --> RADIUS
P-GW ---> Interim accounting response --> RADIUS
```



NOTE: Modify bearer requests are generated by subscriber location information changes, QoS changes, roaming, time-zone changes, and so on.

The following RADIUS logs show how these Interim Accounting messages are processed. When there is a breakdown in AAA communications, the logs help you isolate the cause of the problem.

1. Access the RADIUS log, enable trace options, and look for Authentication and Accounting messages.

Jun 24 11:58:28 879452 gtid:[25]tid: [1] **Accounting-Request**

...

Jun 24 11:58:28 880542 gtid:[25]tid: [1] **Acct-Status-Type [40] 4 0000 0003**

...

Jun 24 11:58:28 880818 gtid:[25]tid: [1] **Acct-Input-Octets [42] 4 0000 00064** <- Data flow

...

Jun 24 11:58:28 880849 gtid:[25]tid: [1] **Acct-Output-Octets [43] 4 0000 00064** <- Data flow

...

Jun 24 11:58:28 891299 gtid:[25]tid: [1] **Accounting-Response**

Accounting stop (delete) requests communicate with the S-GW, the P-GW, and the RADIUS server in the following manner:

```
S-GW --> Delete Session request --> P-GW
P-GW --> Accounting Stop request --> RADIUS
S-GW <-- Delete Session response <-- P-GW
S-GW <-- Delete Session request <-- P-GW
P-GW --> Accounting Sstop --> RADIUS
```

For a dynamic stop request, the flow is:

```
P-GW <-- Disconnect request <-- RADIUS
S-GW <-- Delete Session request <-- P-GW
P-GW --> Accounting Stop --> RADIUS
```

The following RADIUS logs show how these Delete Accounting messages are processed. When there is a breakdown in AAA communications, the logs help you isolate the cause of the problem.

1. Access the RADIUS log, enable trace options, and look for Accounting Stop messages.

```
Jun 24 12:06:29 957706 gtid:[25]tid: [1] jsimRadius(1) Accounting-Request
IP 10.10.2.11 20025 >
```

...

```
Jun 24 12:06:29 958502 gtid:[25]tid: [1] Acct-Status-Type [40] 4 0000
0002
```

...

```
Jun 24 12:06:29 958785 gtid:[25]tid: [1] Acct-Input-Octets [42] 4 0000
00c8 <- Data flow
```

...

```
Jun 24 12:06:29 958815 gtid:[25]tid: [1] Acct-Output-Octets [43] 4 0000
00c8 <- Data flow
```

...

```
Jun 24 12:06:29 974810 gtid:[26]tid: [2] Accounting-Response
```



NOTE: In the displays in this section, **acct-status-type** ends with a four-digit code. The last number of this code is meaningful. A code that ends in 0001 means the process is starting. A code that ends in 0002 means the process is stopping. A code that ends in 0003 means the process is in an interim state, which allows parameters to be changed.

The following aggregate show commands are useful for troubleshooting AAA processes.

- To show AAA statistics authentication details for a specific interface:

```
user@host> show unified-edge ggsn-pgw aaa statistics authentication detail fpc-slot 3 pic-slot 0
```
- To show AAA statistics accounting details for a specific interface:

```
user@host> show unified-edge ggsn-pgw aaa statistics accounting detail fpc-slot 3 pic-slot 0
```
- To show AAA statistics authentication details for a specific PIC:

```
user@host> show unified-edge ggsn-pgw aaa statistics authentication detail
```
- To show AAA statistics accounting details for a specific PIC:

```
user@host> show unified-edge ggsn-pgw aaa statistics accounting detail
```
- To show AAA statistics accounting details for a specific RADIUS server interface:

```
user@host> show unified-edge ggsn-pgw aaa statistics radius authentication detail fpc-slot 3 pic-slot 0 name jsimRadius
```
- To show AAA statistics accounting details for a specific RADIUS server interface:

```
user@host> show unified-edge ggsn-pgw aaa radius statistics accounting detail fpc-slot 3 pic-slot 0 name jsimRadius
```
- To show network element status lists of the RADIUS servers and their status:

```
user@host> show unified-edge ggsn-pgw aaa network-element status name ne1 fpc-slot 3 pic-slot 0
```

```
Network-element: ne1
Server: radius1, Priority: 1, State: Active
Server: radius2, Priority: 1, State: Active
Server: radius3, Priority: 2, State: Active
```

The following clear commands are useful for detecting ongoing activity:

- To clear AAA authentication statistics:

```
user@host> clear unified-edge ggsn-pgw aaa statistics authentication
```
- To clear AAA accounting statistics:

```
user@host> clear unified-edge ggsn-pgw aaa statistics accounting
```
- To clear RADIUS server authentication statistics:

```
user@host> clear unified-edge ggsn-pgw aaa radius statistics authentication
```
- To clear RADIUS server accounting statistics:

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

The following test commands are useful for debugging problems:

- To test user authentication:

```
user@host> test unified-edge ggsn-pgw aaa authentication fpc-slot 1 pic-slot 0 profile abc charging-id 0xfffff username aaa password aaa
```
- To start an accounting test:


```
user@host> test unified-edge ggsn-pgw aaa accounting fpc-slot 1 pic-slot 0 profile  
abc charging-id 0xffffffff start
```

- To stop the accounting test:

```
user@host> test unified-edge ggsn-pgw aaa accounting fpc-slot 1 pic-slot 0 profile  
abc charging-id 0xffffffff stop
```

- To test the interim interval configuration:

```
user@host> test unified-edge ggsn-pgw aaa accounting fpc-slot 1 pic-slot 0 profile abc  
charging-id 0xffffffff interim
```


PART 10

Examples

- [Example Configurations on page 471](#)

CHAPTER 16

Example Configurations

- [Example: Simple Unified Edge Configuration on page 471](#)
- [Example: Configuring MobileNext Broadband Gateway on page 479](#)
- [Example: Configuring MobileNext Broadband Gateway with Provider Edge Functionality on page 507](#)
- [Example: Configuring NAT on page 516](#)
- [Example: Configuring a Standalone S-GW on page 519](#)
- [Example: Configuring a Collocated P-GW and S-GW on page 525](#)
- [Example: Configuring a Multigateway P-GW and S-GW on page 535](#)

Example: Simple Unified Edge Configuration

This example describes how to configure a simple unified edge, and consists of the following sections:

- [Requirements on page 471](#)
- [Overview and Topology on page 471](#)
- [Configuration on page 472](#)
- [Verification on page 478](#)

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 48 on page 472 shows the MobileNext Broadband Gateway components used in this solution.

Table 48: 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	gn interface lo0.0 v4-address 99.1.1.1 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	unit 16000 —Unit required for outgoing packets. unit 0 —One unit required for each APN destination.
Mobile address assignment pool	default-ipv4-address-pool	network 29.0.0.0/8 —Subnet for address assignment to user equipment. range r1 —Named address range. low 29.0.0.1 —Lowest address available. high 29.255.255.254 —Highest address available.

Configuration

To configure a simple unified edge environment, perform the following tasks:

- [Configuring the Hardware Components for Mobility on page 473](#)
- [Configuring the Interface to the Gn Side on page 474](#)

- [Configuring the Mobile Interface Units for Mobility Support on page 475](#)
- [Configuring the Address Pool for Assigning IP Addresses to the User Equipment on page 476](#)
- [Configuring the GGSN Parameters on page 477](#)

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.

Results Check the results of the configuration:

```
root@host> show configuration chassis
fpc 2 {
  forwarding-packages {
    mobility ggsn-pgw;
  }
}
fpc 3 {
  pic 0 {
    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;
        }
      }
    }
  }
  pic 1 {
    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;
        }
      }
    }
  }
}
```

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
[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 {
```

Configuring the GGSN Parameters

```
[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
```

1. Define the broadband gateway as P-GW.

```
[edit unified-edge gateways ggsn-pgw PGW]
user@host# set home-plmn mcc 421 mnc 342
```

```
[edit unified-edge gateways ggsn-pgw PGW gtp ]
user@host# set gn interface lo0.0 v4-address 99.1.1.1
```

```
user@host# edit unified-edge
user@host# show
unified-edge {
    mobile-gateways {
        gateway 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 478](#)
- [Verifying the Gateway Configuration on page 478](#)

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 {
    inactive: mcc 365 mnc 840;
    inactive: mcc 365 mnc 84;
    mcc 421 mnc 342;
```

- Related Documentation
- [Configuring GTP Services Overview on page 226](#)
 - [Configuring a Local Policy on page 343](#)
 - [Configuring GTP Trace Options on page 247](#)
 - [Configuring GTP Services on the Gn Interface on page 236](#)
 - [Configuring a Loopback Interface for Transport of GTP Packets on page 228](#)

Example: Configuring MobileNext Broadband Gateway

This example describes how to configure the MobileNext Broadband Gateway without any provider edge functionality.

- [Requirements on page 479](#)
- [Overview on page 479](#)
- [Configuration on page 481](#)
- [Verification on page 498](#)

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 49: Components of the Broadband Gateway

Property	Settings	Description
Loopback address	lo0 11.11.11.1/32	Identifies the device for communications.

Table 49: Components of the Broadband Gateway (*continued*)

Property	Settings	Description
Routing protocol	isis bgp group	Indicates the device is using IS-IS and BGP as routing protocols.
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 family iso family mpls	The logical units of the core interfaces belong to family inet, family iso, and 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	
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 481](#)
- [Configuring the IPv4 Interfaces on page 482](#)
- [Enabling IS-IS on page 483](#)
- [Enabling MPLS and RSVP Routing on page 484](#)
- [Configuring BGP on page 485](#)
- [Enabling the Routing Instance for the Layer 3 VPN on page 485](#)
- [Configuring RADIUS Servers on page 486](#)
- [Configuring DHCP Proxy Clients on page 486](#)
- [Enabling the APN Configuration on page 487](#)
- [Configuring Offline Charging on page 490](#)
- [Configuring GTP Services on page 494](#)
- [Configuring AAA on page 495](#)
- [Configuring APN Parameters on page 496](#)

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 11.11.11.1/32
set interfaces lo0 unit 3 family inet address 11.11.11.1/32
set interfaces lo0 unit 11 family inet address 11.11.11.1/32
set interfaces lo0 unit 12 family inet address 11.11.11.1/32
set interfaces lo0 unit 13 family inet address 11.11.11.1/32
```

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 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 11.11.11.1/32
user@pe1# set interfaces lo0 unit 3 family inet address 11.11.11.1/32
user@pe1# set interfaces lo0 unit 11 family inet address 11.11.11.1/32
user@pe1# set interfaces lo0 unit 12 family inet address 11.11.11.1/32
user@pe1# set interfaces lo0 unit 13 family inet address 11.11.11.1/32
```

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.mO1REclKM8"
set access radius servers radius_server source-interface lo0.11
set access radius servers radius_server source-interface ipv4-address 11.11.11.1
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 11.11.11.1
```

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
set routing-instances DHCP interface mif.2
```

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
user@pe1# set routing-instances DHCP interface mif.2
```

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
```

[illegible]

```

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
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.102.0.0/16 range r2 low 100.102.0.0
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.102.0.0/16 range r2 high 100.102.255.255
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family inet
network 100.103.0.0/16 range r2 low 100.103.0.0
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.103.0.0/16 range r2 high 100.103.255.255
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.104.0.0/16 range r2 low 100.104.0.0
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.104.0.0/16 range r2 high 100.104.255.255
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.105.0.0/16 range r2 low 100.105.0.0
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.105.0.0/16 range r2 high 100.105.255.255
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.106.0.0/16 range r2 low 100.106.0.0
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.106.0.0/16 range r2 high 100.106.255.255
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.107.0.0/16 range r2 low 100.107.0.0
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.107.0.0/16 range r2 high 100.107.255.255

```

```

user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.108.0.0/16 range r2 low 100.108.0.0
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.108.0.0/16 range r2 high 100.108.255.255
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.109.0.0/16 range r2 low 100.109.0.0
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.109.0.0/16 range r2 high 100.109.255.255
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.110.0.0/16 range r2 low 100.110.0.0
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.110.0.0/16 range r2 high 100.110.255.255
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.111.0.0/16 range r2 low 100.111.0.0
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.111.0.0/16 range r2 high 100.111.255.255
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.112.0.0/16 range r2 low 100.112.0.0
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.112.0.0/16 range r2 high 100.112.255.255
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.113.0.0/16 range r2 low 100.113.0.0
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.113.0.0/16 range r2 high 100.113.255.255
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.114.0.0/16 range r2 low 100.114.0.0
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.114.0.0/16 range r2 high 100.114.255.255
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.115.0.0/16 range r2 low 100.115.0.0
user@pe1# set access address-assignment mobile-pools wireless-juniper1 family
inet network 100.115.0.0/16 range r2 high 100.115.255.255
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_cgf
set unified-edge gateways ggsn-pgw MBG1 charging transport-profiles CGW-trans-pro-1
offline charging-gateways peer-order peer local_cgw
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 gtpv transport-protocol tcp
set unified-edge gateways ggsn-pgw MBG1 charging gtpv version v0
set unified-edge gateways ggsn-pgw MBG1 charging gtpv header-type long
set unified-edge gateways ggsn-pgw MBG1 charging gtpv peer local_cgwr
destination-ipv4-address 42.42.0.2
set unified-edge gateways ggsn-pgw MBG1 charging gtpv peer local_cgwr source-interface
lo0.2
set unified-edge gateways ggsn-pgw MBG1 charging gtpv peer local_cgwr source-interface
ipv4-address 11.11.11.1
set unified-edge gateways ggsn-pgw MBG1 charging gtpv peer local_cgwr destination-port
3386
set unified-edge gateways ggsn-pgw MBG1 charging gtpv peer local_cgwr transport-protocol
tcp
set unified-edge gateways ggsn-pgw MBG1 charging gtpv peer local_cgwr n3-requests 1
set unified-edge gateways ggsn-pgw MBG1 charging gtpv peer local_cgwr t3-response 3
set unified-edge gateways ggsn-pgw MBG1 charging gtpv peer local_cgwr header-type long
set unified-edge gateways ggsn-pgw MBG1 charging gtpv peer local_cgwr
pending-queue-size 1000
set unified-edge gateways ggsn-pgw MBG1 charging gtpv peer my_cgfr
destination-ipv4-address 41.41.0.2
set unified-edge gateways ggsn-pgw MBG1 charging gtpv peer my_cgfr source-interface
lo0.12
set unified-edge gateways ggsn-pgw MBG1 charging gtpv peer my_cgfr source-interface
ipv4-address 11.11.11.1
set unified-edge gateways ggsn-pgw MBG1 charging gtpv peer my_cgfr destination-port
3386
set unified-edge gateways ggsn-pgw MBG1 charging gtpv peer my_cgfr transport-protocol
tcp
set unified-edge gateways ggsn-pgw MBG1 charging gtpv peer my_cgfr n3-requests 1
set unified-edge gateways ggsn-pgw MBG1 charging gtpv peer my_cgfr t3-response 5
set unified-edge gateways ggsn-pgw MBG1 charging gtpv peer my_cgfr header-type long
set unified-edge gateways ggsn-pgw MBG1 charging gtpv peer my_cgfr 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_cgw destination-ipv4-address 42.42.0.2
user@pe1# set gtp peer local_cgw source-interface lo0.2
user@pe1# set gtp peer local_cgw source-interface ipv4-address 11.11.11.1
user@pe1# set gtp peer local_cgw destination-port 3386
user@pe1# set gtp peer local_cgw transport-protocol tcp
user@pe1# set gtp peer local_cgw n3-requests 1
user@pe1# set gtp peer local_cgw t3-response 3
user@pe1# set gtp peer local_cgw header-type long
user@pe1# set gtp peer local_cgw pending-queue-size 1000
user@pe1# set gtp peer my_cgfw destination-ipv4-address 41.41.0.2
user@pe1# set gtp peer my_cgfw source-interface lo0.12
user@pe1# set gtp peer my_cgfw source-interface ipv4-address 11.11.11.1
user@pe1# set gtp peer my_cgfw destination-port 3386
user@pe1# set gtp peer my_cgfw transport-protocol tcp
user@pe1# set gtp peer my_cgfw n3-requests 1
user@pe1# set gtp peer my_cgfw t3-response 5
user@pe1# set gtp peer my_cgfw header-type long
user@pe1# set gtp peer my_cgfw 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_cgfw
user@pe1# set transport-profiles CGW-trans-pro-1 offline charging-gateways
peer-order peer local_cgfw
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 trig-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.
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]
user@pe1# edit unified-edge gateways ggsn-pgw MBG1 gtp
```

```
[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: 199611
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: Sendbcst-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: Sendbcast-pkt-to-re

Meaning The **show interfaces mif.number extensive** command displays detailed information about the specified mobile interface.

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 507](#)
- [Overview on page 507](#)
- [Configuration on page 509](#)
- [Verification on page 514](#)

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 50: Components of the Broadband Gateway

Property	Settings	Description
Loopback address	lo0 unit 100 address 192.168.100.1/32	Interfaces used for 3GPP signaling and IP routing functions
	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	
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 509](#)
- [Configuring the MPLS/BGP VPN on page 510](#)
- [Enabling the Routing Instances for the VPN on page 511](#)
- [Configuring GTP Interfaces on page 512](#)
- [Configuring the Source Interface for RADIUS and Charging Servers on page 513](#)
- [Enabling the APN Configuration on page 513](#)

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.

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 516](#)
- [Overview on page 516](#)
- [Configuration on page 517](#)
- [Verification on page 519](#)

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 517](#)
- [Configuring NAT Pools and NAT Rules on page 518](#)
- [Configuring Service Sets on page 518](#)

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	<p>To configure service sets:</p> <ol style="list-style-type: none"> 1. Configure the service interface associated with the service set. <pre>[edit] user@pe1# set interfaces ms-1/1/0 unit 0 family inet</pre> 2. Configure the service set. <pre>[edit] user@pe1# set services service-set set_0</pre> 3. Specify the NAT rules. <pre>[edit] user@pe1# set services service-set set_0 nat-rules rule_nat44</pre> 4. Specify the service interface. <pre>[edit] user@pe1# set services service-set set_0 interface-service service-interface ms-1/1/0</pre> 5. Associate the service set with the mobile interface. <pre>[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</pre>
-------------------------------	---

Verification

Verifying the NAT Pool Information

Purpose	Verify information about NAT pools.
Action	<pre>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</pre>

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 a full device configuration requires.

- [Requirements on page 519](#)
- [Overview on page 520](#)
- [Configuration on page 520](#)

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 520](#)
- [Configuring the IPv4 Interfaces on page 521](#)
- [Configuring Offline Charging on page 522](#)
- [Configuring System Anchors on page 524](#)
- [Configuring GTP Services on page 524](#)

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 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@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 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 Multiservice 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 anchor-pfes interface pfe-1/0/0
set unified-edge gateways sgw SGW-MBG1 system anchor-spics interface ms-5/0/0
```

Step-by-Step Procedure To configure the anchor packet forwarding engine and service PIC:

1. Configure the anchor packet forwarding engine.

```
[edit unified-edge gateways sgw SGW-MBG1 system]
user@sgw1# set anchor-pfes interface pfe-1/0/0
```
2. Configure the anchor service PIC.

```
[edit unified-edge gateways sgw SGW-MBG1 system]
user@sgw1# set anchor-spics 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 60
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 60
```

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 60
user@sgw1# set s11 echo-n3-requests 5
user@sgw1# set s11 echo-t3-response 60

```

- Related Documentation**
- [Example: Configuring a Multigateway P-GW and S-GW on page 535](#)
 - [Example: Configuring a Collocated P-GW and S-GW on page 525](#)

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 a full device configuration requires.

- [Requirements on page 525](#)
- [Overview on page 525](#)
- [Configuration on page 526](#)

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 526](#)
- [Configuring Charging for the P-GW on page 528](#)
- [Configuring Charging for the S-GW on page 530](#)
- [Configuring System Anchors for the broadband gateway S-GW and P-GW on page 532](#)
- [Configuring GTP Services for the P-GW and S-GW on page 533](#)
- [Configure the APNs for the P-GW on page 534](#)

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 Multiservice 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-ie-options 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_cg
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

```
3. 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_cfg destination-ipv4-address 10.3.3.3
user@pgw-sgw-1# set gtp peer my_cfg source-interface lo0.0
user@pgw-sgw-1# set gtp peer my_cfg source-interface ipv4-address 10.9.88.1
user@pgw-sgw-1# set gtp peer my_cfg destination-port 3386
user@pgw-sgw-1# set gtp peer my_cfg transport-protocol udp
user@pgw-sgw-1# set gtp peer my_cfg n3-requests 1
user@pgw-sgw-1# set gtp peer my_cfg t3-response 5
user@pgw-sgw-1# set gtp peer my_cfg header-type short
user@pgw-sgw-1# set gtp peer my_cfg pending-queue-size 1000

```

4. 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-ie-options
    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
```

5. 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_cfg t3-response 3
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 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 service 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 service 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 service 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

```

Related Documentation

- [Example: Configuring a Multigateway P-GW and S-GW on page 535](#)
- [Example: Configuring a Standalone S-GW on page 519](#)

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 a full device configuration requires.

- [Requirements on page 536](#)
- [Overview on page 536](#)
- [Configuration on page 537](#)

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 537](#)
- [Configuring Charging for the P-GWs on page 539](#)
- [Configuring Charging for the S-GWs on page 542](#)
- [Configuring System Anchors for the broadband gateway P-GWs named PGW1-MBG1 and PGW2-MBG2 on page 546](#)
- [Configuring System Anchors for the broadband gateway S-GWs named SGW1-MBG1 and SGW2-MBG1 on page 546](#)
- [Configuring GTP Services for the P-GWs named PGW1-MBG1 and PGW2-MBG2 on page 547](#)
- [Configuring GTP Services for the S-GWc named SGW1-MBG1 and SGW2-MBG1 on page 548](#)
- [Configure the APNs for the P-GW on page 549](#)

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 Multiservice 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 gtpv peer p_cfg t3-response
5
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging gtpv peer p_cfg header-type
long
set unified-edge gateways ggsn-pgw PGW1-MBG1 charging gtpv 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 gtpv transport-protocol tcp
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging gtpv version v0
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging gtpv header-type long
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging gtpv peer p_cfg
destination-ipv4-address 10.2.2.2
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging gtpv peer p_cfg source-interface
ms-3/1/0.0
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging gtpv peer p_cfg source-interface
ipv4-address 10.4.1.4
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging gtpv peer p_cfg destination-port
3386
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging gtpv peer p_cfg
transport-protocol tcp
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging gtpv peer p_cfg n3-requests
1
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging gtpv peer p_cfg t3-response
5
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging gtpv peer p_cfg header-type
long
set unified-edge gateways ggsn-pgw PGW2-MBG1 charging gtpv 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_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 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_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 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_cfg
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_cfgfw 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_cfg destination-ipv4-address 10.2.2.2
user@pgw-sgw-1# set gtp peer p_cfg source-interface ms-5/1/0.0
user@pgw-sgw-1# set gtp peer p_cfg source-interface ipv4-address 10.4.1.2
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 version v0
user@pgw-sgw-1# set gtp peer p_cfgfw 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 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 service 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 service 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 service 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 service 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 service 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 service 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 61
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 61
```

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 61
```

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 61
```

Configuring GTP Services for the S-GWc 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 slu echo-n3-requests 5
set unified-edge gateways sgw SGW1-MBG1 gtp slu echo-t3-response 60
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 slu echo-n3-requests 5
set unified-edge gateways sgw SGW2-MBG1 gtp slu echo-t3-response 60
```

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 sll echo-n3-requests 5
user@pgw-sgw-1# set sll echo-t3-responses 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 sll echo-n3-requests 5
user@pgw-sgw-1# set sll echo-t3-responses 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
```

- Related Documentation**
- [Example: Configuring a Collocated P-GW and S-GW on page 525](#)
 - [Example: Configuring a Standalone S-GW on page 519](#)

PART 11

Complete Configuration Statement Hierarchy and Summary of Statements

- [Configuration Statement Hierarchy on page 553](#)
- [AAA on the Broadband Gateway on page 585](#)
- [Address Assignment and DHCP Configuration Statements on page 617](#)
- [Anchor Packet Forwarding Engine Redundancy and Aggregated Multiservices High Availability Configuration Statements on page 645](#)
- [APN Configuration Statements on page 677](#)
- [Charging Configuration Statements on page 769](#)
- [Class of Service \(CoS\) Configuration Statements on page 855](#)
- [Exception Handling Configuration Statements on page 897](#)
- [Gateway Maintenance Mode Configuration Statement on page 915](#)
- [GTP Configuration Statements on page 917](#)
- [Service Applications Configuration Statements on page 971](#)
- [System Architecture and Gateway Traceoptions Configuration Statements on page 981](#)

Configuration Statement Hierarchy

- [\[edit access\] Hierarchy Level on page 553](#)
- [\[edit access address-assignment\] Hierarchy Level on page 554](#)
- [\[edit class-of-service\] Hierarchy Level on page 555](#)
- [\[edit interfaces ams\] Hierarchy Level on page 555](#)
- [\[edit interfaces apfe\] Hierarchy Level on page 556](#)
- [\[edit interfaces mif\] Hierarchy Level on page 557](#)
- [\[edit routing-instance system\] Hierarchy Level on page 557](#)
- [\[edit services hcm\] Hierarchy Level on page 558](#)
- [\[edit services ip-reassembly\] Hierarchy Level on page 559](#)
- [\[edit services service-set\] Hierarchy Level on page 559](#)
- [\[edit unified-edge\] Hierarchy Level on page 559](#)
- [\[edit unified-edge aaa\] Hierarchy Level on page 560](#)
- [\[edit unified-edge cos-cac\] Hierarchy Level on page 561](#)
- [\[edit unified-edge gateways\] Hierarchy Level on page 563](#)
- [\[edit unified-edge gateways ggsn-pgw <gateway-name>\] Hierarchy Level on page 564](#)
- [\[edit unified-edge gateways sgw <gateway-name>\] Hierarchy Level on page 574](#)
- [\[edit unified-edge local-policies\] Hierarchy Level on page 582](#)
- [\[edit unified-edge mobile-options\] Hierarchy Level on page 582](#)
- [\[edit unified-edge resource-management\] Hierarchy Level on page 582](#)

[\[edit access\] Hierarchy Level](#)

```
access {  
  radius {  
    traceoptions {  
      file radius;  
      flag send-detail;  
      flag rcv-detail;  
      level all;  
      server {  
        server name;  
      }  
    }  
  }  
}
```

```
    }
    servers server-name {
        address address;
        source-interface interface {
            ipv4-address address;
        }
        accounting-port port-number;
        accounting-secret password;
        allow-dynamic-requests ;
        authentication-port port-number;
        dead-criteria retries retry-number interval seconds;
        dynamic-requests-secret password;
        retry attempts;
        revert-interval time;
        secret password;
        timeout seconds;
    }
}
network-elements name {
    server name {
        priority priority ;
    }
    algorithm ( direct | round-robin);
    maximum-pending-reqs-limit number ;
}
network-element-groups name {
    network-element name {
        mandatory;
    }
    broadcast;
}
}
```

Related Documentation

- [Notational Conventions Used in Junos OS Configuration Hierarchies](#)

[edit access address-assignment] Hierarchy Level

```
address-assignment {
    mobile-pool-groups {
        group-name {
            [pool-name];
        }
    }
    mobile-pools {
        name {
            ageing-window ageing-window;
            default-pool;
            family (inet | inet6) {
                network {
                    [network-prefix] {
                        external-assigned;
                    }
                }
            }
        }
    }
}
```



```

range {
  [name] {
    external-assigned;
    high high;
    low low;
  }
}
}
}
}
}
pool-prefetch-threshold pool-prefetch-threshold;
pool-snmp-trap-threshold pool-snmp-trap-threshold;
service-mode service-mode-options;
}
}
}

```

Related Documentation • [Notational Conventions Used in Junos OS Configuration Hierarchies](#)

[\[edit class-of-service\] Hierarchy Level](#)

```

class-of-service {
  interfaces {
    mif. number {
      rewrite-rules {
        dscp rewrite-rule-name [protocol gtp-inet-both|gtp-inet-outer];
        dscp-ipv6 rewrite-rule-name [protocol gtp-inet-both|gtp-inet-outer];
        inet-precedence rewrite-rule-name [protocol gtp-inet-both|gtp-inet-outer];
      }
      ingress-rewrite-rules {
        dscp rewrite-rule-name;
        dscp-ipv6 rewrite-rule-name;
        inet-precedence rewrite-rule-name;
      }
    }
  }
}

```

Related Documentation • [Notational Conventions Used in Junos OS Configuration Hierarchies](#)

[\[edit interfaces ams\] Hierarchy Level](#)

```

interfaces amsx {
  hold-time {
    ...
  }
  layer2-policer {
    ...
  }
  load-balancing-options {
    high-availability-options {
      many-to-one {
        preferred-backup preferred-backup;

```

```
    }
  }
  member-failure-options {
    drop-member-traffic {
      rejoin-timeout rejoin-timeout;
    }
    redistribute-all-traffic {
      enable-rejoin;
    }
  }
  member-interface interface-name;
}
multi-chassis-protection {
  ...
}
services-options {
  ...
}
traceoptions {
  ...
}
unit interface-unit-number {
  dial-options {
    (dedicated | shared);
    ipsec-interface-id ipsec-interface-id;
  }
  family family;
  load-balancing-options {
    preferred-active interface-name;
  }
}
}
```

Related Documentation

- [Notational Conventions Used in Junos OS Configuration Hierarchies](#)

[edit interfaces apfe] Hierarchy Level

```
interfaces apfex {
  anchoring-options {
    apfe-group-set apfe-group-set;
    primary-list {
      [anchoring-device-name];
    }
    secondary anchoring-device-name;
    warm-standby;
  }
  hold-time {
    ...
  }
  layer2-policer {
    ...
  }
  multi-chassis-protection {
    ...
  }
}
```

```

    }
    traceoptions {
        ...
    }
}

```

Related Documentation • [Notational Conventions Used in Junos OS Configuration Hierarchies](#)

[edit interfaces mif] Hierarchy Level

```

interfaces mif {
    description description;
    disable;
    mtu mtu-size;
    multi-chassis-protection { ... }
    no-traps;
    traceoptions { ... }
    unit interface-unit-number {
        clear-dont-fragment-bit;
        description description;
        disable;
        family family-name { ... }
        filter {
            input input-filter;
            output output-filter;
        }
        (no-traps | traps);
    }
}

```

Related Documentation • [Notational Conventions Used in Junos OS Configuration Hierarchies](#)

[edit routing-instance system] Hierarchy Level

```

services {
    dhcp-proxy-client {
    }
    dhcpv4-profiles profile-name {
        bind-interface interface-name ip-address;
        dead-server-retry-interval n seconds;
        dead-server-successive-retry-attempt number-of-attempts;
        dhcp-server-selection-algorithm (highest-priority-server | round-robin);
        lease-time n seconds;
        pool-name strings;
        retransmission-attempt number-of-attempts;
        retransmission-interval n seconds;
        server {
            ipv4-address priority value;
        }
    }
}
    dhcpv6-profiles profile-name {
        bind-interface interface-name ip-address;
        dead-server-retry-interval n seconds;
    }
}

```

```
    dead-server-successive-retry-attempt number-of-attempts;  
    dhcp-server-selection-algorithm (highest-priority-server | round-robin);  
    lease-time n seconds;  
    pool-name strings;  
    retransmission-attempt number-of-attempts;  
    retransmission-interval n seconds;  
    server {  
        ipv6-address priority value ;  
    }  
}  
}  
trace-options {  
    file ;  
    flag ;  
}  
}
```

Related Documentation

- [Notational Conventions Used in Junos OS Configuration Hierarchies](#)

[edit services hcm] Hierarchy Level

```
hcm {  
    tag-attribute [attr-name];  
    tag-rule rule-name {  
        term term-name {  
            from {  
                destination-address {  
                    (any-unicast | any-unicast except);  
                    [prefix];  
                }  
                destination-address-range {  
                    [high address low address] [except];  
                }  
                destination-port-range {  
                    [high port-number low port-number];  
                }  
                destination-ports [value];  
                destination-prefix-list {  
                    (prefix-name | prefix-name except);  
                }  
            }  
        }  
        then {  
            count;  
            tag tag-name {  
                encrypt {  
                    hash algorithm;  
                    prefix hash-prefix;  
                }  
                tag-attribute tag-attr-name;  
                tag-header header;  
                tag-separator separator;  
            }  
        }  
    }  
}
```

```

    }
    tag-rule-set rule-set-name {
        [rule rule-name];
    }
}

```

Related Documentation • [Notational Conventions Used in Junos OS Configuration Hierarchies](#)

[\[edit services ip-reassembly\] Hierarchy Level](#)

```

ip-reassembly profile-name {
    max-reassembly-pending-packets number;
    timeout in-seconds;
}

```

Related Documentation • [Notational Conventions Used in Junos OS Configuration Hierarchies](#)

[\[edit services service-set\] Hierarchy Level](#)

```

service-set service-set-name {
    interface-service {
        load-balancing-options {
            hash-keys {
                egress-key (destination-ip | source-ip);
                ingress-key (destination-ip | source-ip);
                resource-triggered;
            }
        }
        service-interface interface-name.unit-number;
    }
    [tag-rule-sets rule-set-name];
    [tag-rules rule-name];
    service-set-options {
        subscriber-awareness;
    }
}

```

Related Documentation • [Notational Conventions Used in Junos OS Configuration Hierarchies](#)

[\[edit unified-edge\] Hierarchy Level](#)

Each of the following topics lists the statements at a subhierarchy of the **[edit unified-edge]** hierarchy.

- [\[edit unified-edge aaa\] Hierarchy Level on page 560](#)
- [\[edit unified-edge cos-cac\] Hierarchy Level on page 561](#)
- [\[edit unified-edge gateways\] Hierarchy Level on page 563](#)
- [\[edit unified-edge local-policies\] Hierarchy Level on page 582](#)

- [\[edit unified-edge mobile-options\] Hierarchy Level on page 582](#)
- [\[edit unified-edge resource-management\] Hierarchy Level on page 582](#)

Related Documentation • [Notational Conventions Used in Junos OS Configuration Hierarchies](#)

[edit unified-edge aaa] Hierarchy Level

```
unified-edge {
  aaa {
    traceoptions {
    }
    mobile-profiles {
      map-name {
        radius {
          authentication {
            network-element name;
          }
          accounting {
            network-element name;
            network-element-group group-name;
            stop-on-failure;
            stop-on-access-deny;
            send-accounting-on;
            trigger {
              interim-interval minutes;
              no-cos-change;
              no-deferred-ipv4-address-update;
              no-ms-timezone-change;
              no-plmn-change;
              no-rat-change;
              no-sgw-change;
              no-user-location-information-change;
            }
          }
        }
      }
      options {
        nas-identifier-prefix identifier-value;
      }
      attributes {
        ignore {
          output-filter;
          framed-ip-netmask;
          input-filter;
        }
        exclude {
          accounting-authentic [accounting-start | accounting-interim |
            accounting-stop];
          accounting-delay-time [accounting-start | accounting-interim |
            accounting-stop];
          accounting-terminate-cause [accounting-stop];
          all-3gpp [access-request | accounting-start | accounting-stop |
            accounting-interim];
          called-station-id [access-request | accounting-start | accounting-interim |
            accounting-stop];
        }
      }
    }
  }
}
```

```

calling-station-id [access-request | accounting-start | accounting-interim |
  accounting-stop];
charging-id [access-request | accounting-interim | accounting-start |
  accounting-stop];
event-timestamp [accounting-start | accounting-interim | accounting-stop];
ggsn-address [access-request | accounting-interim | accounting-start |
  accounting-stop];
gprs-negotiated-qos [access-request | accounting-interim | accounting-start
  | accounting-stop];
imeisv [access-request | accounting-start];
imsi [access-request | accounting-start | accounting-stop |
  accounting-interim];
imsi-mcc-mnc [access-request | accounting-start | accounting-stop |
  accounting-interim];
input-gigapackets [accounting-interim | accounting-stop];
input-gigawords [accounting-interim | accounting-stop];
input-packets [accounting-interim | accounting-stop];
nas-identifier [access-request | accounting-interim | accounting-start
  | accounting-stop];
nas-ip-address [access-request | accounting-on | accounting-off |
  accounting-start | accounting-interim | accounting-stop];
nas-port-type [access-request | accounting-interim | accounting-start |
  accounting-stop];
nsapi [access-request | accounting-interim | accounting-start |
  accounting-stop];
output-gigapackets [accounting-interim | accounting-stop];
output-gigawords [accounting-interim | accounting-stop];
output-packets [accounting-interim | accounting-stop];
selection-mode [access-request | accounting-interim | accounting-start |
  accounting-stop];
sgsn-mcc-mnc [access-request | accounting-start | accounting-interim |
  accounting-stop];
user-location-info [access-request | accounting-start | accounting-stop |
  accounting-interim];
}
}
}
}
}
}
}
}
}
}

```

- Related Documentation**
- [\[edit unified-edge\] Hierarchy Level on page 559](#)
 - [Notational Conventions Used in Junos OS Configuration Hierarchies](#)

[\[edit unified-edge cos-cac\] Hierarchy Level](#)

```

unified-edge {
  cos-cac {
    classifier-profiles {
      name {
        traffic-class-classifier-profiles conversational | streaming | background
        forwarding-class fc-name loss-priority [low | high];
      }
    }
  }
}

```

```

traffic-class-classifier-profiles interactive traffic-handling-priority 1 | 2 | 3
    forwarding-class fc-name loss-priority [low | high];
    qos-class-identifier x forwarding-class fc-name loss-priority [low | high];
}
}
bandwidth-pools {
    name {
        bandwidth x;
        traffic-class-bandwidth-pool conversational | streaming percentage z downgrade
        ;
    }
}
resource-threshold-profiles {
    name {
        system-load {
            low {
                gtpv1-arp y;
                gtpv2-priority-level z;
                percentage x;
            }
            high {
                gtpv1-arp y;
                gtpv2-priority-level z;
                percentage x;
            }
        }
        bearer-load {
            low {
                gtpv1-arp y;
                gtpv2-priority-level z;
                percentage x;
            }
            high {
                gtpv1-arp y;
                gtpv2-priority-level z;
                percentage x;
            }
        }
        cpu {
            low {
                gtpv1-arp y;
                gtpv2-priority-level z;
                percentage x;
            }
            high {
                gtpv1-arp y;
                gtpv2-priority-level z;
                percentage x;
            }
        }
        memory {
            low {
                gtpv1-arp y;
                gtpv2-priority-level z;
                percentage x;
            }
            high {
                gtpv1-arp y;
                gtpv2-priority-level z;
            }
        }
    }
}

```



```

        percentage x;
    }
}
}
cos-policy-profiles {
    name {
        qci 5 to 9 [upgrade];
        traffic-class-cos-policy-profiles string priority z [upgrade];
        aggregated-maximum-bit-rate {
            downlink x;
            reject;
            upgrade;
            uplink y;
        }
        allocation-retention-priority {
            gtpv2-priority-value 1 to 15 [upgrade];
            gtpv1-priority-value 1 to 3 [upgrade];
        }
        maximum-bit-rate {
            traffic-class-cos-policy-profiles {
                any [both] | [uplink] | [downlink] x
                background [both] | [uplink] | [downlink] x
                conversational [both] | [uplink] | [downlink] x
                interactive [both] | [uplink] | [downlink] x
                reject;
                streaming [both] | [uplink] | [downlink] x
                upgrade;
            }
        }
        guaranteed-bit-rate {
            traffic-class-cos-policy-profiles {
                any [both] | [uplink] | [downlink] x
                conversational [both] | [uplink] | [downlink] x
                reject;
                streaming [both] | [uplink] | [downlink] x
                upgrade;
            }
        }
        exceed-action [drop | transmit];
        violate-action [set-loss-priority-high | transmit];
    }
}
}

```

Related
Documentation

- [Notational Conventions Used in Junos OS Configuration Hierarchies](#)

[\[edit unified-edge gateways\] Hierarchy Level](#)

Each of the following topics lists the statements at a sub-hierarchy of the **[edit unified-edge gateways]** hierarchy.

- [\[edit unified-edge gateways ggsn-pgw <gateway-name>\] Hierarchy Level](#) on page 564
- [\[edit unified-edge gateways sgw <gateway-name>\] Hierarchy Level](#) on page 574

- Related Documentation**
- [\[edit unified-edge\] Hierarchy Level on page 559](#)
 - [Notational Conventions Used in Junos OS Configuration Hierarchies](#)

[\[edit unified-edge gateways ggsn-pgw <gateway-name>\] Hierarchy Level](#)

```
ggsn-pgw gateway-name {
  anchor-pfe-ipv4-nbm-prefixes maximum-ipv4-prefixes;
  anchor-pfe-ipv6-nbm-prefixes maximum-ipv6-prefixes;
  apn-services {
    apns {
      [name] {
        aaa-profile aaa-profile;
        address-assignment {
          aaa;
          allow-static-ip-address {
            no-address-verify;
          }
          dhcp-proxy-client {
            aaa-override;
          }
          dhcpv4-proxy-client-profile {
            logical-system logical-system;
            pool-name pool-name;
            profile-name profile-name;
            routing-instance routing-instance;
          }
          dhcpv6-proxy-client-profile {
            logical-system logical-system;
            pool-name pool-name;
            profile-name profile-name;
            routing-instance routing-instance;
          }
        }
        inet-pool {
          exclude-pools [value];
          group group;
          pool pool;
        }
        inet6-pool {
          exclude-v6pools [value];
          group group;
          pool pool;
        }
        local {
          aaa-override;
        }
      }
    }
    allow-network-behind-mobile;
    anonymous-user {
      password password;
      (use-apnname | use-imsi | use-msisdn | user-name username);
    }
    apn-data-type (ipv4 | ipv4v6 | ipv6);
    apn-type (real | virtual | virtual-pre-authenticate);
  }
}
```

```

block-visitors;
charging {
    default-profile default-profile;
    home-profile home-profile;
    profile-selection-order [profile-selection-method];
    roamer-profile roamer-profile;
    visitor-profile visited-profile;
}
description description;
dns-server {
    primary-v4 primary-v4;
    primary-v6 primary-v6;
    secondary-v4 secondary-v4;
    secondary-v6 secondary-v6;
}
idle-timeout idle-timeout;
idle-timeout-direction (both | uplink);
inter-mobile-traffic {
    (deny | redirect redirect);
}
local-policy-profile local-policy-profile;
maximum-bearers maximum-bearers;
mobile-interface mobile-interface;
nbns-server {
    primary-v4 primary-v4;
    secondary-v4 secondary-v4;
}
network-behind-mobile {
    imsi imsi {
        prefix-v4 [ipv4-prefix];
        prefix-v6 [ipv6-prefix];
    }
}
p-cscf {
    [address];
}
restriction-value restriction-value;
selection-mode {
    (from-ms | from-sgsn | no-subscribed);
}
service-mode service-mode-options;
service-selection-profile service-selection-profile;
session-timeout session-timeout;
verify-source-address {
    disable;
}
wait-accounting;
}
}
call-rate-statistics {
    history history;
    interval interval;
}
charging {
    cdr-profiles profile-name {

```

```
description string;  
enable-reduced-partial-cdrs;  
exclude-ie-options {  
    apn-ni;  
    apn-selection-mode;  
    cc-selection-mode;  
    dynamic-address;  
    list-of-service-data;  
    list-of-traffic-volumes;  
    lrsn;  
    ms-time-zone;  
    network-initiation;  
    node-id;  
    pdn-connection-id;  
    pdppdn-type;  
    pgw-address-used; # S-GW only  
    pgw-plmn-identifier;  
    rat-type;  
    record-sequence-number;  
    served-imeisv;  
    served-msisdn;  
    served-pdppdn-address;  
    serving-node-plmn-identifier;  
    sgw-change; # S-GW only  
    start-time;  
    stop-time;  
    user-location-information;  
}  
}  
charging-profiles profile-name {  
    cdr-profile profile-name;  
    default-rating-group rg-num;  
    default-service-id id-num;  
    description string;  
    profile-id id-num;  
    transport-profile profile-name;  
    trigger-profile profile-name;  
    service-mode maintenance;  
}  
gtp {  
    destination-port port-number;  
    down-detect-time duration;  
    echo-interval duration;  
    header-type (long | short);  
    n3-requests requests;  
    no-path-management;  
    pending-queue-size value;  
    peer peer-name {  
        destination-ipv4-address address;  
        destination-port port-number;  
        down-detect-time duration;  
        echo-interval duration;  
        header-type (long | short);  
        n3-requests requests;  
        no-path-management;  
        pending-queue-size value;
```

```

    reconnect-time duration;
    source-interface interface-name [ipv4-address address];
    t3-response response-interval;
    transport-protocol (tcp | udp);
    version (v0 | v1 | v2);
}
reconnect-time duration;
source-interface {
    interface-name;
    ipv4-address address;
}
t3-response response-interval;
transport-protocol (tcp | udp);
version (v0 | v1 | v2);
}
local-persistent-storage-options {
    cdrs-per-file value;
    disable-replication;
    disk-space-policy {
        watermark-level-1 {
            notification-level (both | snmp-alarm | syslog);
            percentage value;
        }
        watermark-level-2 {
            notification-level (both | snmp-alarm | syslog);
            percentage value;
        }
        watermark-level-3 {
            notification-level (both | snmp-alarm | syslog);
            percentage value;
        }
    }
}
file-age value;
file-creation-policy (shared-file | unique-file);
file-format (3gpp | raw-asn);
file-name-private-extension string;
file-size value;
traceoptions {
    file file-name <files number> <match regular-expression> <no-world-readable |
        world-readable> <size size>;
    flag flag;
    level (all | critical | error | info | notice | verbose | warning);
    no-remote-trace;
}
user-name string;
world-readable;
}
traceoptions {
    file file-name <files number> <no-world-readable | world-readable> <size size>;
    flag flag;
    level (all | critical | error | info | notice | verbose | warning);
    no-remote-trace;
}
transport-profiles profile-name {
    description string;
    offline {

```

```

charging-gateways {
  cdr-aggregation-limit value;
  cdr-release (r7 | r8 | r99);
  mtu value;
  peer-order {
    [peer charging-gateway-peer-name];
  }
  persistent-storage-order {
    local-storage;
  }
  switch-back-time seconds;
}
}
service-mode maintenance;
}
trigger-profiles profile-name {
  description string;
  offline {
    container-limit value;
    exclude {
      ms-timezone-change;
      plmn-change;
      qos-change;
      rat-change;
      sgsn-sgw-change;
      user-location-change;
    }
    sgsn-sgw-change-limit value;
    time-limit value;
    volume-limit {
      value;
      direction (both | uplink);
    }
  }
}
tariff-time-list {
  [tariff-time];
}
}
}
gtp {
  control {
    dscp-code-point value;
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    forwarding-class class-name;
    interface {
      interface-name;
      v4-address v4-address;
    }
    n3-requests requests;
    no-response-cache;
    path-management (disable | enable);
    response-cache-timeout interval-in-seconds;
    t3-response response-interval;
  }
}

```

```

data {
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    error-indication-interval seconds;
    interface {
        interface-name;
        v4-address v4-address;
    }
    path-management (disable | enable);
}
echo-interval interval;
echo-n3-requests requests;
echo-t3-response response-interval;
gn {
    control {
        dscp-code-point value;
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        forwarding-class class-name;
        interface {
            interface-name;
            v4-address v4-address;
        }
        n3-requests requests;
        path-management (disable | enable);
        t3-response response-interval;
    }
    data {
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        interface {
            interface-name;
            v4-address v4-address;
        }
        n3-requests requests;
        path-management (disable | enable);
        t3-response response-interval;
    }
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    interface {
        interface-name;
        v4-address v4-address;
    }
    n3-requests requests;
    path-management (disable | enable);
    t3-response response-interval;
}
gp {
    control {
        dscp-code-point value;
        echo-interval interval;

```

```
    echo-n3-requests requests;
    echo-t3-response response-interval;
    forwarding-class class-name;
    interface {
        interface-name;
        v4-address v4-address;
    }
    n3-requests requests;
    path-management (disable | enable);
    t3-response response-interval;
}
data {
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    interface {
        interface-name;
        v4-address v4-address;
    }
    n3-requests requests;
    path-management (disable | enable);
    t3-response response-interval;
}
echo-interval interval;
echo-n3-requests requests;
echo-t3-response response-interval;
interface {
    interface-name;
    v4-address v4-address;
}
n3-requests requests;
path-management (disable | enable);
t3-response response-interval;
}
interface {
    interface-name;
    v4-address v4-address;
}
n3-requests requests;
path-management (disable | enable);
peer-group name {
    control {
        support-16-bit-sequence;
    }
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    n3-requests requests;
    path-management (disable | enable);
    peer {
        [ip-addr-prefix];
    }
    routing-instance routing-identifier;
    t3-response response-interval;
}
peer-history number;
```



```

s5 {
  control {
    dscp-code-point value;
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    forwarding-class class-name;
    interface {
      interface-name;
      v4-address v4-address;
    }
    n3-requests requests;
    path-management (disable | enable);
    support-16-bit-sequence;
    t3-response response-interval;
  }
  data {
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    interface {
      interface-name;
      v4-address v4-address;
    }
    n3-requests requests;
    path-management (disable | enable);
    t3-response response-interval;
  }
  echo-interval interval;
  echo-n3-requests requests;
  echo-t3-response response-interval;
  interface {
    interface-name;
    v4-address v4-address;
  }
  n3-requests requests;
  path-management (disable | enable);
  t3-response response-interval;
}
s8 {
  control {
    dscp-code-point value;
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    forwarding-class class-name;
    interface {
      interface-name;
      v4-address v4-address;
    }
    n3-requests requests;
    path-management (disable | enable);
    support-16-bit-sequence;
    t3-response response-interval;
  }
  data {

```

```
    echo-interval interval;  
    echo-n3-requests requests;  
    echo-t3-response response-interval;  
    interface {  
        interface-name;  
        v4-address v4-address;  
    }  
    n3-requests requests;  
    path-management (disable | enable);  
    t3-response response-interval;  
}  
echo-interval interval;  
echo-n3-requests requests;  
echo-t3-response response-interval;  
interface {  
    interface-name;  
    v4-address v4-address;  
}  
n3-requests requests;  
path-management (disable | enable);  
t3-response response-interval;  
}  
t3-response response-interval;  
traceoptions {  
    file filename {  
        files files;  
        (no-world-readable | world-readable);  
        size size;  
    }  
    flag {  
        flag;  
    }  
    level level;  
    no-remote-trace;  
}  
}  
home-plmn {  
    mcc [mcc] {  
        mnc [mnc];  
    }  
}  
ip-reassembly-profile {  
    profile-name;  
}  
ipv6-router-advertisement {  
    current-hop-limit current-hop-limit;  
    disable;  
    maximum-advertisement-interval maximum-advertisement-interval;  
    maximum-initial-advertisement-interval maximum-initial-advertisement-interval;  
    maximum-initial-advertisements maximum-initial-advertisements;  
    minimum-advertisement-interval minimum-advertisement-interval;  
    reachable-time reachable-time;  
    retransmission-timer retransmission-timer;  
    router-lifetime router-lifetime;  
}  
local-policy-profile local-policy-profile;
```

```

maximum-bearers maximum-bearers;
preemption {
    enable;
    gtpv1-pci-disable;
    gtpv1-pvi-disable;
}
service-mode maintenance;
service-selection-profiles {
    profile name {
        term name {
            from {
                charging-characteristics charging-characteristics;
                imei imei;
                imsi imsi;
                maximum-bearers maximum-bearers;
                msisdn msisdn;
                pdn-type (ipv4 | ipv4v6 | ipv6);
                peer peer;
                peer-routing-instance peer-routing-instance;
            }
            then {
                apn-name apn-name;
                redirect-peer redirect-peer;
            }
        }
    }
}
software-datapath {
    traceoptions {
        file filename {
            files files;
            match match;
            size size;
            (no-world-readable | world-readable);
        }
        flag {
            flag;
        }
        level level;
        no-remote-trace;
    }
}
system {
    anchor-pfes {
        [interface interface-name];
    }
    anchor-service-pics {
        [interface interface-name];
    }
    anchor-spics {
        [interface interface-name];
    }
}
traceoptions {
    file filename {
        files files;

```

```
    match match;  
    (no-world-readable | world-readable);  
    size size;  
  }  
  flag {  
    flag;  
  }  
  level level;  
  no-remote-trace;  
}  
}
```

- Related Documentation**
- [\[edit unified-edge gateways\] Hierarchy Level on page 563](#)
 - [Notational Conventions Used in Junos OS Configuration Hierarchies](#)

[edit unified-edge gateways sgw <gateway-name>] Hierarchy Level

```
sgw gateway-name {  
  anchor-pfe-default-bearers-percentage default-bearers-percentage;  
  anchor-pfe-guaranteed-bandwidth anchor-pfe-guaranteed-bandwidth;  
  anchor-pfe-maximum-bearers maximum-bearers;  
  call-rate-statistics {  
    history history;  
    interval interval;  
  }  
  charging {  
    cdr-profiles profile-name {  
      description string;  
      enable-reduced-partial-cdrs;  
      exclude-ie-options {  
        apn-ni;  
        apn-selection-mode;  
        cc-selection-mode;  
        dynamic-address;  
        list-of-service-data;  
        list-of-traffic-volumes;  
        lrsn;  
        ms-time-zone;  
        network-initiation;  
        node-id;  
        pdn-connection-id;  
        pdppdn-type;  
        pgw-address-used;  
        pgw-plmn-identifier;  
        rat-type;  
        record-sequence-number;  
        served-imeisv;  
        served-msisdn;  
        served-pdppdn-address;  
        serving-node-plmn-identifier;  
        sgw-change;  
        start-time;  
        stop-time;  
        user-location-information;  
      }  
    }  
  }  
}
```

```

    }
  }
  charging-profiles profile-name {
    cdr-profile profile-name;
    default-rating-group rg-num;
    default-service-id id-num;
    description string;
    profile-id id-num;
    transport-profile profile-name;
    trigger-profile profile-name;
    service-mode maintenance;
  }
  global-profile {
    default-profile default-profile;
    home-profile home-profile;
    profile-selection-order [profile-selection-method];
    roamer-profile roamer-profile;
    visitor-profile visitor-profile;
  }
  gtp {
    destination-port port-number;
    down-detect-time duration;
    echo-interval duration;
    header-type (long | short);
    n3-requests requests;
    no-path-management;
    pending-queue-size value;
    peer peer-name {
      destination-ipv4-address address;
      destination-port port-number;
      down-detect-time duration;
      echo-interval duration;
      header-type (long | short);
      n3-requests requests;
      no-path-management;
      pending-queue-size value;
      reconnect-time duration;
      source-interface interface-name [ipv4-address address];
      t3-response response-interval;
      transport-protocol (tcp | udp);
      version (v0 | v1 | v2);
    }
    reconnect-time duration;
    source-interface {
      interface-name;
      ipv4-address address;
    }
    t3-response response-interval;
    transport-protocol (tcp | udp);
    version (v0 | v1 | v2);
  }
  local-persistent-storage-options {
    cdrs-per-file value;
    disable-replication;
    disk-space-policy {
      watermark-level-1 {

```

```

        notification-level (both | snmp-alarm | syslog);
        percentage value;
    }
    watermark-level-2 {
        notification-level (both | snmp-alarm | syslog);
        percentage value;
    }
    watermark-level-3 {
        notification-level (both | snmp-alarm | syslog);
        percentage value;
    }
}
file-age value;
file-creation-policy (shared-file | unique-file);
file-format (3gpp | raw-asn);
file-name-private-extension string;
file-size value;
traceoptions {
    file file-name <files number> <match regular-expression> <no-world-readable |
    world-readable> <size size>;
    flag flag;
    level (all | critical | error | info | notice | verbose | warning);
    no-remote-trace;
}
user-name string;
world-readable;
}
traceoptions {
    file file-name <files number> <no-world-readable | world-readable> <size size>;
    flag flag;
    level (all | critical | error | info | notice | verbose | warning);
    no-remote-trace;
}
transport-profiles profile-name {
    description string;
    offline {
        charging-gateways {
            cdr-aggregation-limit value;
            cdr-release (r7 | r8 | r99);
            mtu value;
            peer-order {
                [peer charging-gateway-peer-name];
            }
            persistent-storage-order {
                local-storage;
            }
            switch-back-time seconds;
        }
    }
    service-mode maintenance;
}
trigger-profiles profile-name {
    description string;
    offline {
        container-limit value;
        exclude {

```

```

        ms-timezone-change;
        plmn-change;
        qos-change;
        rat-change;
        sgsn-mme-change;
        user-location-change;
    }
    sgsn-mme-change-limit value;
    time-limit value;
    volume-limit {
        value;
        direction (both | uplink);
    }
}
tariff-time-list {
    [tariff-time];
}
}
}
gtp {
    control {
        ddns-delay-sync (disable | enable);
        dscp-code-point value;
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        forwarding-class class-name;
        interface {
            interface-name;
            v4-address v4-address;
        }
        n3-requests requests;
        no-response-cache;
        path-management (disable | enable);
        response-cache-timeout interval-in-seconds;
        t3-response response-interval;
        ttl-value ttl-value;
    }
    data {
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        error-indication-interval seconds;
        indirect-tunnel (disable | enable);
        interface {
            interface-name;
            v4-address v4-address;
        }
        num-gtpu-end-markers num-gtpu-end-markers;
        path-management (disable | enable);
    }
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    interface {
        interface-name;

```

```
    v4-address v4-address;
  }
  n3-requests requests;
  path-management (disable | enable);
  peer-history number;
  s11 {
    dscp-code-point value;
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    interface {
      interface-name;
      v4-address v4-address;
    }
    n3-requests requests;
    path-management (disable | enable);
    t3-response response-interval;
    ttl-value ttl-value;
  }
  s12 {
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    interface {
      interface-name;
      v4-address v4-address;
    }
    path-management (disable | enable);
  }
  slu {
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    interface {
      interface-name;
      v4-address v4-address;
    }
    path-management (disable | enable);
  }
  s4 {
    control {
      dscp-code-point value;
      echo-interval interval;
      echo-n3-requests requests;
      echo-t3-response response-interval;
      forwarding-class class-name;
      interface {
        interface-name;
        v4-address v4-address;
      }
      n3-requests requests;
      path-management (disable | enable);
      t3-response response-interval;
      ttl-value ttl-value;
    }
    data {
```



```

    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    interface {
        interface-name;
        v4-addressv4-address;
    }
    path-management (disable | enable);
}
echo-interval interval;
echo-n3-requests requests;
echo-t3-response response-interval;
interface {
    interface-name;
    v4-addressv4-address;
}
n3-requests requests;
path-management (disable | enable);
t3-response response-interval;
}
s5 {
    control {
        dscp-code-point value;
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        forwarding-class class-name;
        interface {
            interface-name;
            v4-addressv4-address;
        }
        n3-requests requests;
        path-management (disable | enable);
        t3-response response-interval;
        ttl-value ttl-value;
    }
    data {
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        interface {
            interface-name;
            v4-addressv4-address;
        }
        path-management (disable | enable);
    }
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    interface {
        interface-name;
        v4-addressv4-address;
    }
    n3-requests requests;
    path-management (disable | enable);
    t3-response response-interval;
}

```

```
}
s8 {
  control {
    dscp-code-point value;
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    forwarding-class class-name;
    interface {
      interface-name;
      v4-addressv4-address;
    }
    n3-requests requests;
    path-management (disable | enable);
    t3-response response-interval;
    ttl-value ttl-value;
  }
  data {
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    interface {
      interface-name;
      v4-addressv4-address;
    }
    path-management (disable | enable);
  }
  echo-interval interval;
  echo-n3-requests requests;
  echo-t3-response response-interval;
  interface {
    interface-name;
    v4-addressv4-address;
  }
  n3-requests requests;
  path-management (disable | enable);
  t3-response response-interval;
}
t3-response response-interval;
traceoptions {
  file filename {
    files files;
    (no-world-readable | world-readable);
    size size;
  }
  flag {
    flag;
  }
  level level;
  no-remote-trace;
}
}
home-plmn {
  mcc [mcc] {
    mnc [mnc];
  }
}
```

```

}
idle-mode-buffering {
    disable;
    expire-timer time-in-seconds;
}
ip-reassembly-profile {
    profile-name;
}
local-policy-profile local-policy-profile;
maximum-bearers maximum-bearers;
preemption {
    enable;
}
remote-delete-on-peer-fail;
service-mode
software-datapath {
    traceoptions {
        file filename {
            files files;
            match match;
            size size;
            (no-world-readable | world-readable);
        }
        flag {
            flag;
        }
        level level;
        no-remote-trace;
    }
}
system {
    anchor-pfes {
        [interface interface-name];
    }
    anchor-spics {
        [interface interface-name];
    }
}
traceoptions {
    file filename {
        files files;
        match match;
        (no-world-readable | world-readable);
        size size;
    }
    flag {
        flag;
    }
    level level;
    no-remote-trace;
}
}

```

- Related Documentation**
- [\[edit unified-edge gateways\] Hierarchy Level on page 563](#)
 - [Notational Conventions Used in Junos OS Configuration Hierarchies](#)

[edit unified-edge local-policies] Hierarchy Level

```
unified-edge {  
  local-policies {  
    name {  
      cos-policy-profile name;  
      classifier-profile name;  
      dl-bandwidth-pool name;  
      roamer-classifier-profile name;  
      roamer-cos-policy-profile name;  
      resource-threshold-profiles name;  
      ul-bandwidth-pool name;  
      visitor-classifier-profile name;  
      visitor-cos-policy-profile name;  
    }  
  }  
}
```

- Related Documentation**
- [\[edit unified-edge\] Hierarchy Level on page 559](#)
 - [Notational Conventions Used in Junos OS Configuration Hierarchies](#)

[edit unified-edge mobile-options] Hierarchy Level

```
unified-edge {  
  mobile-options {  
    traceoptions {  
      file filename {  
        files files;  
        match match;  
        (no-world-readable | world-readable);  
        size size;  
      }  
      flag {  
        flag;  
      }  
      no-remote-trace;  
    }  
  }  
}
```

- Related Documentation**
- [\[edit unified-edge\] Hierarchy Level on page 559](#)
 - [Notational Conventions Used in Junos OS Configuration Hierarchies](#)

[edit unified-edge resource-management] Hierarchy Level

```
unified-edge {  
  resource-management {  
    client {  
      traceoptions {  
        file filename {
```

```

        files files;
        match match;
        (no-world-readable | world-readable);
        size size;
    }
    flag {
        flag;
    }
    no-remote-trace;
}
server {
    traceoptions {
        file filename {
            files files;
            match match;
            (no-world-readable | world-readable);
            size size;
        }
        flag {
            flag;
        }
        no-remote-trace;
    }
}
}
}

```

**Related
Documentation**

- [\[edit unified-edge\] Hierarchy Level on page 559](#)
- [Notational Conventions Used in Junos OS Configuration Hierarchies](#)

CHAPTER 18

AAA on the Broadband Gateway

aaa

```
Syntax  aaa {
    traceoptions {
    }
    mobile-profiles {
        map-name {
            radius {
                authentication {
                    network-element name;
                }
                accounting {
                    network-element name;
                    network-element-group group-name;
                    stop-on-failure;
                    stop-on-access-deny;
                    send-accounting-on;
                    trigger {
                        interim-interval minutes;
                        no-cos-change;
                        no-deferred-ipv4-address-update;
                        no-ms-timezone-change;
                        no-plmn-change;
                        no-rat-change;
                        no-sgw-change;
                        no-user-location-information-change;
                    }
                }
            }
        }
        options {
            nas-identifier-prefix identifier-value;
        }
        attributes {
            ignore {
                output-filter;
                framed-ip-netmask;
                input-filter;
            }
            exclude {
                accounting-authentic [accounting-start | accounting-interim | accounting-stop];
                accounting-delay-time [accounting-start | accounting-interim |
                    accounting-stop];
                accounting-terminate-cause [accounting-stop];
                all-3gpp [access-request | accounting-start | accounting-stop |
                    accounting-interim];
                called-station-id [access-request | accounting-start | accounting-interim |
                    accounting-stop];
                calling-station-id [access-request | accounting-start | accounting-interim |
                    accounting-stop];
                cg-address [access-request | accounting-start | accounting-stop |
                    accounting-interim];
                event-timestamp [accounting-start | accounting-interim | accounting-stop];
                imeisv [access-request | accounting-start];
                imsi [access-request | accounting-start | accounting-stop | accounting-interim];
            }
        }
    }
}
```



```

imsi-mcc-mnc [access-request | accounting-start | accounting-stop |
  accounting-interim];
input-filter [accounting-start | accounting-stop];
input-gigapackets [accounting-interim | accounting-stop];
input-gigawords [accounting-stop];
nas-identifier [access-request | accounting-start | accounting-interim |
  accounting-stop];
nas-ip-address [access-request |
  accounting-on|accounting-off|accounting-start | accounting-interim |
  accounting-stop];
nas-port [access-request | accounting-start | accounting-stop];
nas-port-id [access-request | accounting-start | accounting-interim |
  accounting-stop];
nas-port-type [access-request];
output-filter [accounting-start | accounting-stop];
output-gigapackets [accounting-interim | accounting-stop];
output-gigawords [accounting-stop];
sgsn-mcc-mnc [access-request | accounting-start | accounting-interim |
  accounting-stop];
user-location-info [access-request | accounting-start | accounting-stop |
  accounting-interim];
}
}
}
}
}
}

```

Hierarchy Level [edit unified-edge]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the authentication, authorization, and accounting (AAA) services provided using groups of external RADIUS servers. The Broadband Gateway supports a framework for providing AAA services to mobile subscribers.

Options The remaining statements are explained separately.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation • [Overview of AAA on the Broadband Gateway on page 148](#)

accounting

Syntax accounting {
 network-element *name*;
 network-element-group *group-name*;
 stop-on-failure;
 stop-on-access-deny;
 send-accounting-on;
 trigger {
 no-cos-change;
 no-deferred-ipv4-address-update;
 no-ms-timezone-change;
 no-plmn-change;
 no-rat-change;
 no-sgw-change;
 no-user-location-information-change;
 }
 }

Hierarchy Level [edit unified-edge aaa mobile-profiles *map-name* radius]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify RADIUS accounting-related parameters. You can specify either the network element or the network element group to which the accounting requests are sent. In addition, the triggers that can initiate interim accounting records to be sent can be controlled.

The remaining statements are explained separately.

Required Privilege Level access—To view this statement in the configuration.
 access-control—To add this statement to the configuration.

Related Documentation

- [Overview of AAA on the Broadband Gateway on page 148](#)
- [radius on page 606](#)

accounting-port

Syntax	<code>accounting-port <i>port-number</i>;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> radius-server <i>server-address</i>], [edit access radius-server <i>server-address</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the port number on which to contact the accounting server.
Options	<i>port-number</i> —Port number on which to contact the accounting server. Most RADIUS servers use port number 1813 (as specified in RFC 2866).
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Overview of AAA on the Broadband Gateway on page 148 • servers on page 610

accounting-secret

Syntax	<code>accounting-secret <i>password</i>;</code>
Hierarchy Level	[edit access radius servers <i>server-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the secret password to be used when sending accounting requests to the RADIUS server. If the secret password is different from the authentication secret password, specify the accounting secret by using this option.
Default	Use the same password used for authentication requests.
Options	<i>password</i> —Password for accounting requests.
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Overview of AAA on the Broadband Gateway on page 148 • servers on page 610

address

Syntax	<code>address <i>address</i>;</code>
Hierarchy Level	<code>[edit access radius servers <i>server-name</i>]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the IPv4 address of the RADIUS server to which the authentication and accounting requests are sent.
Options	<i>address</i> —IPv4 address of the RADIUS server.
Required Privilege Level	<code>access</code> —To view this statement in the configuration. <code>access-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Overview of AAA on the Broadband Gateway on page 148• servers on page 610

algorithm

Syntax	<code>algorithm (<i>direct</i> <i>round-robin</i>);</code>
Hierarchy Level	<code>[edit access radius network-elements <i>name</i>]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify an algorithm to decide which RADIUS server is used for the next request.
Options	<i>direct</i> —Default method in which there is no load balancing. The gateway always uses the highest-priority server to send requests. The other servers are used as backup. <i>round-robin</i> —This method provides for load balancing in which the gateway sends requests to different high-priority servers in a rotating fashion. Lower-priority servers are used as backup.
Required Privilege Level	<code>access</code> —To view this statement in the configuration. <code>access-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Overview of AAA on the Broadband Gateway on page 148• network-elements on page 602

allow-dynamic-requests

Syntax	allow-dynamic-requests;
Hierarchy Level	[edit access radius servers <i>server-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify this option to receive dynamic requests from the RADIUS server.
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Overview of AAA on the Broadband Gateway on page 148• servers on page 610

attributes

```
Syntax  attributes {
        ignore {
            output-filter;
            framed-ip-netmask;
            input-filter;
        }
        exclude {
            accounting-authentic [accounting-start | accounting-interim | accounting-stop];
            accounting-delay-time [accounting-start | accounting-interim | accounting-stop];
            accounting-terminate-cause [accounting-stop];
            all-3gpp [access-request | accounting-start | accounting-stop | accounting-interim];
            called-station-id [access-request | accounting-start | accounting-interim |
                accounting-stop];
            calling-station-id [access-request | accounting-start | accounting-interim |
                accounting-stop];
            cg-address [access-request | accounting-start | accounting-stop | accounting-interim];
            event-timestamp [accounting-start | accounting-interim | accounting-stop];
            imeisv [access-request | accounting-start];
            imsi [access-request | accounting-start | accounting-stop | accounting-interim];
            imsi-mcc-mnc [access-request | accounting-start | accounting-stop |
                accounting-interim];
            input-filter [accounting-start | accounting-stop];
            input-gigapackets [accounting-interim | accounting-stop];
            input-gigawords [accounting-stop];
            nas-identifier [access-request | accounting-start | accounting-interim |
                accounting-stop];
            nas-ip-address [access-request | accounting-on|accounting-off|accounting-start |
                accounting-interim | accounting-stop];
            nas-port [access-request | accounting-start | accounting-stop];
            nas-port-id [access-request | accounting-start | accounting-interim | accounting-stop];
            nas-port-type [access-request];
            output-filter [accounting-start | accounting-stop];
            output-gigapackets [accounting-interim | accounting-stop];
            output-gigawords [accounting-stop];
            sgsn-mcc-mnc [access-request | accounting-start | accounting-interim |
                accounting-stop];
            user-location-info [access-request | accounting-start | accounting-stop |
                accounting-interim];
        }
    }
```

Hierarchy Level [edit unified-edge aaa mobile-profiles *map-name* radius]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the RADIUS attributes to be ignored by the broadband gateway in Access-Accept messages that the AAA profile receives. You can also specify which RADIUS attributes must be excluded by the gateway from specific types of RADIUS messages that the AAA profile generates.

The remaining statements are explained separately.

Required Privilege access—To view this statement in the configuration.
Level access-control—To add this statement to the configuration.

Related Documentation

- [Overview of AAA on the Broadband Gateway on page 148](#)
- [radius on page 606](#)

authentication

Syntax authentication {
 network-element *name*;
 }

Hierarchy Level [edit unified-edge aaa mobile-profiles *map-name* radius]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the network element to be used for authentication. If the network element is not specified, authentication requests for the access point name (APN) pointing to that profile is not be triggered.

Required Privilege access—To view this statement in the configuration.
Level access-control—To add this statement to the configuration.

Related Documentation

- [Overview of AAA on the Broadband Gateway on page 148](#)
- [radius on page 606](#)

authentication-port

Syntax authentication-port *port-number*;

Hierarchy Level [edit access radius servers *server-name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the port number to which the RADIUS authentication requests are sent.

Default The default port number is 1812.

Options *port-number*—Port number to which the RADIUS authentication requests are sent.

Required Privilege access—To view this statement in the configuration.
Level access-control—To add this statement to the configuration.

Related Documentation

- [Overview of AAA on the Broadband Gateway on page 148](#)
- [servers on page 610](#)

dead-criteria-retries

Syntax	<code>dead-criteria retries <i>retry-number</i> interval <i>seconds</i>;</code>
Hierarchy Level	<code>[edit access radius servers <i>server-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 11.2.
Description	Specify the criteria used to mark a RADIUS server dead. If the number of retries exceeds the <i>retry-number</i> within an interval of <i>seconds</i> , then the RADIUS server is marked dead.
Default	If this attribute value is not specified, then the dead server detection option is disabled.
Options	<i>retry-number</i> —Number of retries with set values. <i>seconds</i> —Time interval in seconds.
Required Privilege Level	<code>access</code> —To view this statement in the configuration. <code>access-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Overview of AAA on the Broadband Gateway on page 148• servers on page 610

dynamic-requests-secret

Syntax	<code>dynamic-requests-secret <i>password</i>;</code>
Hierarchy Level	<code>[edit access radius servers <i>server-name</i>]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the secret password used for dynamic requests. The secret password has to be specified to receive dynamic requests from the RADIUS server.
Default	Use the same password that is used for authentication requests.
Options	<i>password</i> —Password for dynamic requests.
Required Privilege Level	<code>access</code> —To view this statement in the configuration. <code>access-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Overview of AAA on the Broadband Gateway on page 148• servers on page 610

exclude (RADIUS)

```
Syntax  exclude {
    accounting-authentic [accounting-start | accounting-interim | accounting-stop];
    accounting-delay-time [accounting-start | accounting-interim | accounting-stop];
    accounting-terminate-cause [accounting-stop];
    all-3gpp [access-request | accounting-start | accounting-stop | accounting-interim];
    called-station-id [access-request | accounting-start | accounting-interim | accounting-stop];
    calling-station-id [access-request | accounting-start | accounting-interim |
        accounting-stop];
    charging-id [access-request | accounting-interim | accounting-start | accounting-stop];
    event-timestamp [accounting-start | accounting-interim | accounting-stop];
    ggsn-address [access-request | accounting-interim | accounting-start | accounting-stop];
    gprs-negotiated-qos [access-request | accounting-interim | accounting-start |
        accounting-stop];
    imeisv [access-request | accounting-start];
    imsi [access-request | accounting-start | accounting-stop | accounting-interim];
    imsi-mcc-mnc [access-request | accounting-start | accounting-stop | accounting-interim];
    input-gigapackets [accounting-interim | accounting-stop];
    input-gigawords [accounting-interim | accounting-stop];
    input-packets [accounting-interim | accounting-stop];
    nas-identifier [access-request | accounting-interim | accounting-start | accounting-stop];
    nas-ip-address [access-request | accounting-on | accounting-off | accounting-start |
        accounting-interim | accounting-stop];
    nas-port-type [access-request | accounting-interim | accounting-start | accounting-stop];
    nsapi [access-request | accounting-interim | accounting-start | accounting-stop];
    output-gigapackets [accounting-interim | accounting-stop];
    output-gigawords [accounting-interim | accounting-stop];
    output-packets [accounting-interim | accounting-stop];
    selection-mode [access-request | accounting-interim | accounting-start | accounting-stop];
    sgsn-mcc-mnc [access-request | accounting-start | accounting-interim | accounting-stop];
    user-location-info [access-request | accounting-start | accounting-stop |
        accounting-interim];
}
```

Hierarchy Level [edit unified-edge aaa mobile-profiles *map-name* radius attributes]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.
Support for the **charging-id**, **ggsn-address**, **gprs-negotiated-qos**, **nsapi**, and **selection-mode** attributes introduced in Junos OS Mobility Release 11.4W.

Description Configure the gateway to exclude the specified attributes from the specified type of RADIUS message.

Not all attributes are available in all types of RADIUS messages. By default, the gateway includes the specified attributes in RADIUS Access-Request, Acct-On, Acct-Off, Acct-Start, and Acct-Stop messages.

Options RADIUS attribute type—RADIUS attribute or Juniper Networks VSA number and name.

- **accounting-authentic**—Exclude the RADIUS attribute 45, Acct-Authentic.
- **accounting-delay-time**—Exclude the RADIUS attribute 41, Acct-Delay-Time.

- **accounting-terminate-cause**—Exclude the RADIUS attribute 49, Acct-Terminate-Cause.
- **all-3gpp**—Exclude all 3GPP attributes.
- **called-station-id**—Exclude the RADIUS attribute 30, Called-Station-ID.
- **calling-station-id**—Exclude the RADIUS attribute 31, Calling-Station-ID.
- **charging-id**—Exclude the RADIUS attribute 3GPP VSA 26-2, 3GPP-CHARGING-ID.
- **event-timestamp**—Exclude the RADIUS attribute 55, Event-Timestamp.
- **ggsn-address**—Exclude the RADIUS attribute 3GPP VSA 26-7, 3GPP-GGSN-ADDRESS.
- **gprs-negotiated-qos**—Exclude the RADIUS attribute 3GPP VSA 26-5, 3GPP-GPRS-NEG-QOS.
- **imei**—Exclude the 3GPP-IMEISV attribute from the access-request or accounting-start request sent to the RADIUS server.
- **imsi**—Exclude the 3GPP-IMSI attribute from the requests sent to the RADIUS server.
- **imsi-mcc-mnc**—Exclude the RADIUS attribute 3GPP VSA 26-8, 3GPP-IMSI-MCC-MNC.
- **input-gigapackets**—Exclude the RADIUS attribute 26-42, Acct-Input-Gigapackets.
- **input-gigawords**—Exclude the RADIUS attribute 52, Acct-Input-Gigawords.
- **input-packets**—Exclude the RADIUS attribute 47, Acct-Input-Packets.
- **nas-identifier**—Exclude the RADIUS attribute 32, NAS-identifier.
- **nas-ip-address**—Exclude the RADIUS attribute, NAS-IP-address.
- **nas-port-type**—Exclude the RADIUS attribute 61, NAS-Port-Type.
- **nsapi**—Exclude the RADIUS attribute 3GPP VSA 26-10, 3GPP-NSAPI.
- **output-gigapackets**—Exclude the RADIUS attribute 26-43, Acct-Output-Gigapackets.
- **output-gigawords**—Exclude the RADIUS attribute 53, Acct-Output-Gigawords.
- **output-packets**—Exclude the RADIUS attribute 48, Acct-Output-Packets.
- **selection-mode**—Exclude the RADIUS attribute 3GPP VSA 26-12, 3GPP-SELECTION-MODE.
- **sgsn-mcc-mnc**—Exclude the SGSN-MCC-MNC attribute from the requests sent to the RADIUS server.
- **user-location-info**—Exclude the RADIUS attribute 3GPP VSA 26-22, 3GPP-USER-LOCATION-INFO.

Required Privilege Level	access—To view this statement in the configuration.
	access-control—To add this statement to the configuration.
Related Documentation	• Overview of AAA on the Broadband Gateway on page 148
	• attributes on page 592

ignore

Syntax	ignore { output-filter; framed-ip-netmask; input-filter; }
Hierarchy Level	[edit unified-edge aaa mobile-profiles <i>map-name</i> radius attributes]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure so that the specified attribute in RADIUS Access-Accept messages is ignored.
Options	<p><i>output-filter</i>—Ignore this attribute in the Access-Accept message.</p> <p><i>framed-ip-netmask</i>—Ignore this attribute in the Access-Accept message.</p> <p><i>input-filter</i>—Ignore this attribute in the Access-Accept message.</p>
Required Privilege Level	<p>access—To view this statement in the configuration.</p> <p>access-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Overview of AAA on the Broadband Gateway on page 148 • attributes on page 592

maximum-pending-reqs-limit

Syntax	maximum-pending-reqs-limit <i>number</i> ;
Hierarchy Level	[edit access radius network-elements <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	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, a flow control on message is generated. When the number of pending requests subsequently drops to 60 percent of the maximum, a flow control off message is generated.
Options	<i>number</i> —Maximum number of pending requests.
Required Privilege Level	<p>access—To view this statement in the configuration.</p> <p>access-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Overview of AAA on the Broadband Gateway on page 148 • network-elements on page 602

mobile-profiles

```
Syntax  mobile-profiles {
        map-name {
            radius {
                authentication {
                    network-element name;
                }
                accounting {
                    network-element name;
                    network-element-group group-name;
                    stop-on-failure;
                    stop-on-access-deny;
                    send-accounting-on;
                    trigger {
                        no-rat-change;
                        no-sgw-change;
                        no-cos-change;
                        interim-interval minutes;
                        no-plmn-change;
                        no-user-location-information-change;
                        no-ms-timezone-change;
                        no-deferred-ipv4-address-update;
                    }
                }
            }
            options {
                nas-identifier-prefix identifier-value;
            }
            attributes {
                ignore {
                    output-filter;
                    framed-ip-netmask;
                    input-filter;
                }
                exclude {
                    accounting-authentic [accounting-start | accounting-interim | accounting-stop];
                    accounting-delay-time [accounting-start | accounting-interim | accounting-stop];
                    accounting-terminate-cause [accounting-stop];
                    all-3gpp [access-request | accounting-start | accounting-stop |
                        accounting-interim];
                    called-station-id [access-request | accounting-start | accounting-interim |
                        accounting-stop];
                    calling-station-id [access-request | accounting-start | accounting-interim |
                        accounting-stop];
                    cg-address [access-request | accounting-start | accounting-stop |
                        accounting-interim];
                    event-timestamp [accounting-start | accounting-interim | accounting-stop];
                    imeisv [access-request | accounting-start];
                    imsi [access-request | accounting-start | accounting-stop | accounting-interim];
                    imsi-mcc-mnc [access-request | accounting-start | accounting-stop |
                        accounting-interim];
                    input-filter [accounting-start | accounting-stop];
                    input-gigapackets [accounting-interim | accounting-stop];
                    input-gigawords [accounting-stop];
                }
            }
        }
    }
```

```

        nas-identifier [access-request | accounting-start | accounting-interim |
            accounting-stop];
        nas-ip-address [access-request | accounting-on|accounting-off|accounting-start
            | accounting-interim | accounting-stop];
        nas-port [access-request | accounting-start | accounting-stop];
        nas-port-id [access-request | accounting-start | accounting-interim |
            accounting-stop];
        nas-port-type [access-request];
        output-filter [accounting-start | accounting-stop];
        output-gigapackets [accounting-interim | accounting-stop];
        output-gigawords [accounting-stop];
        sgsn-mcc-mnc [access-request | accounting-start | accounting-interim |
            accounting-stop];
        user-location-info [access-request | accounting-start | accounting-stop |
            accounting-interim];
    }
}
}
}
}

```

Hierarchy Level [edit unified-edge aaa]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the sections under mobile-profiles that control the access and accounting request information sent to the RADIUS server. It also contains sections to specify the network element or network element group to which the request must be sent.

Options The remaining statements are explained separately.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- [Overview of AAA on the Broadband Gateway on page 148](#)
- [aaa on page 586](#)

network-element

Syntax	<code>network-element <i>name</i>;</code>
Hierarchy Level	[edit unified-edge aaa mobile-profiles <i>map-name</i> radius accounting]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the network element to be used for accounting. If the accounting network element is not specified, accounting requests for the access point name pointing to that profile is not be triggered.
Options	<i>name</i> —Name of the network element.
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Overview of AAA on the Broadband Gateway on page 148• accounting on page 588

network-element-group

Syntax	<code>network-element-group <i>group-name</i>;</code>
Hierarchy Level	[edit unified-edge aaa mobile-profiles <i>map-name</i> radius accounting]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the network element group used for accounting. The network element group allows to send the same accounting record to multiple RADIUS network elements. You can specify either a network element or a network element group for accounting.
Options	<i>group-name</i> —Name of the network element group.
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Overview of AAA on the Broadband Gateway on page 148• accounting on page 588

network-element-groups

Syntax	<pre> network-element-groups <i>name</i> { network-element <i>name</i> { mandatory; } broadcast; } </pre>
Hierarchy Level	[edit access radius]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure a group of network elements. A network element group can have a maximum of four network elements. You can optionally configure the broadcast attribute in a network element. However, if broadcast is configured, then there should be a minimum of one network element that is flagged as mandatory. Network element-groups are used for accounting records and is used only for accounting in the AAA profile.</p>
Options	<p><i>mandatory</i>—Indicates that a response is mandatory from a specified network element before any services can be provided to the subscriber.</p> <p><i>broadcast</i>—Broadcasts the accounting messages to all of the network elements in the group. If you configure the broadcast parameter, you should specify the mandatory parameter for at least one of the network elements in the group.</p> <p><i>name</i>—Name of the network element group.</p>
Required Privilege Level	<p>access—To view this statement in the configuration.</p> <p>access-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Overview of AAA on the Broadband Gateway on page 148 • radius on page 604

network-elements

Syntax	<pre>network-elements <i>name</i> { server <i>name</i> { priority <i>priority</i>; } algorithm (<i>direct</i> <i>round-robin</i>); maximum-pending-reqs-limit <i>number</i>; }</pre>
Hierarchy Level	[edit access radius]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify a network element that is a load-balanced group of RADIUS servers providing authentication, authorization, and accounting services for mobile subscribers accessing an APN. The RADIUS servers have two priorities: 1 or 2. You can have multiple servers with the same priority in a network element. All requests are sent to the highest priority server in the network element based on the algorithm (direct or round-robin).
Options	<p><i>name</i>—Name of the network element.</p> <p><i>priority</i>—Relative priority for the first server.</p>
Required Privilege Level	<p>access—To view this statement in the configuration.</p> <p>access-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Overview of AAA on the Broadband Gateway on page 148• radius on page 604

options

Syntax	<pre>options { nas-identifier-prefix <i>identifier-value</i> nas-ip-address <i>gw-address</i>; nas-port-type <i>type</i>; }</pre>
Hierarchy Level	[edit unified-edge aaa mobile-profiles <i>map-name</i> radius]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the attributes that are included as part of different request messages sent to the RADIUS server.
Options	<p>nas-identifier-prefix <i>identifier-value</i>—Specify the prefix that is used in the NAS identifier attribute. Each services PIC appends a unique suffix and that appended value will be used as the NAS identifier in the RADIUS requests.</p> <p>nas-ip-address <i>gw-address</i>—The IP address to be used for the NAS IP address attribute when sending the requests to the RADIUS server.</p> <p>nas-port-type <i>type</i>—The NAS port type (wireless or virtual) that is used in RADIUS requests.</p>
Required Privilege Level	<p>access—To view this statement in the configuration.</p> <p>access-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Overview of AAA on the Broadband Gateway on page 148 • radius on page 606

radius (Access)

```
Syntax  radius {
        traceoptions {
            file radius;
            flag send-detail;
            flag recv-detail;
            level all;
            server {
                server name;
            }
        }
        servers server-name {
            address address;
            source-interface interface {
                ipv4-address address;
            }
            accounting-port port-number;
            accounting-secret password;
            allow-dynamic-requests ;
            authentication-port port-number;
            dead-criteria retries retry-number interval seconds;
            dynamic-requests-secret password;
            retry attempts;
            revert-interval time;
            secret password;
            timeout seconds;
        }
        network-elements name {
            server name {
                priority priority ;
            }
            algorithm ( direct | round-robin );
            maximum-pending-reqs-limit number ;
        }
        network-element-groups name {
            network-element name {
                mandatory;
            }
            broadcast;
        }
    }
```

Hierarchy Level [edit access]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify multiple RADIUS servers with their attributes. The RADIUS servers are distinguished by unique names. You can also group a set of RADIUS servers into a network element. A network element is a load-balanced group of RADIUS servers that provides authentication, authorization, and accounting services for mobile subscribers accessing

an access point name. Additionally, you can group a set of network elements into a network element-group.

Options *name*—Name of the server.

The remaining statements are explained separately.

Required Privilege access—To view this statement in the configuration.
Level access-control—To add this statement to the configuration.

Related • [Overview of AAA on the Broadband Gateway on page 148](#)
Documentation

radius

```
Syntax  radius {
    authentication {
        network-element name;
    }
    accounting {
        network-element name;
        network-element-group group-name;
        stop-on-failure;
        stop-on-access-deny;
        send-accounting-on;
        trigger {
            no-rat-change;
            no-sgw-change;
            no-cos-change;
            interim-interval minutes;
            no-plmn-change;
            no-user-location-information-change;
            no-ms-timezone-change;
            no-deferred-ipv4-address-update;
        }
    }
    options {
        nas-identifier-prefix identifier-value;
    }
    attributes {
        ignore {
            output-filter;
            framed-ip-netmask;
            input-filter;
        }
        exclude {
            accounting-authentic [accounting-start | accounting-interim | accounting-stop];
            accounting-delay-time [accounting-start | accounting-interim | accounting-stop];
            accounting-terminate-cause [accounting-stop];
            all-3gpp [access-request | accounting-start | accounting-stop | accounting-interim];
            called-station-id [access-request | accounting-start | accounting-interim |
                accounting-stop];
            calling-station-id [access-request | accounting-start | accounting-interim |
                accounting-stop];
            cg-address [access-request | accounting-start | accounting-stop |
                accounting-interim];
            event-timestamp [accounting-start | accounting-interim | accounting-stop];
            imeisv [access-request | accounting-start];
            imsi [access-request | accounting-start | accounting-stop | accounting-interim];
            imsi-mcc-mnc [access-request | accounting-start | accounting-stop |
                accounting-interim];
            input-filter [accounting-start | accounting-stop];
            input-gigapackets [accounting-interim | accounting-stop];
            input-gigawords [accounting-stop];
            nas-identifier [access-request | accounting-start | accounting-interim |
                accounting-stop];
```

```

    nas-ip-address [access-request | accounting-on|accounting-off|accounting-start |
        accounting-interim | accounting-stop];
    nas-port [access-request | accounting-start | accounting-stop];
    nas-port-id [access-request | accounting-start | accounting-interim |
        accounting-stop];
    nas-port-type [access-request];
    output-filter [accounting-start | accounting-stop];
    output-gigapackets [accounting-interim | accounting-stop];
    output-gigawords [accounting-stop];
    sgsn-mcc-mnc [access-request | accounting-start | accounting-interim |
        accounting-stop];
    user-location-info [access-request | accounting-start | accounting-stop |
        accounting-interim];
}
}
}

```

Hierarchy Level	[edit unified-edge]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify multiple RADIUS servers with their attributes. The RADIUS servers are distinguished with unique names.
Options	The remaining statements are explained separately.
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Overview of AAA on the Broadband Gateway on page 148 • aaa on page 586

retry

Syntax	<code>retry <i>attempts</i>;</code>
Hierarchy Level	<code>[edit access radius servers <i>server-name</i>]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the number of attempts that the gateway is allowed to contact a RADIUS authentication or accounting server when it does not receive a response to its initial request.
Options	<i>attempts</i> —Number of attempts that the gateway is allowed to contact a RADIUS server. Range: 1 through 10 Default: 3
Required Privilege Level	access —To view this statement in the configuration. access-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Overview of AAA on the Broadband Gateway on page 148• servers on page 610

revert-interval

Syntax	<code>revert-interval <i>time</i>;</code>
Hierarchy Level	<code>[edit access radius servers <i>server-name</i>]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the amount of time the gateway waits after a server has become unreachable. After the configured time, the server is marked active and is used to send requests in accordance with its order and priority in the network element.
Options	<i>time</i> —Duration after which a dead server is marked active. Default: 300 seconds
Required Privilege Level	access —To view this statement in the configuration. access-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Overview of AAA on the Broadband Gateway on page 148• servers on page 610

secret

Syntax	<code>secret password;</code>
Hierarchy Level	[edit access radius servers <i>server-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify a default password to be used for authentication or accounting. This is a mandatory statement.
Options	<i>password</i> —Password to use.
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Overview of AAA on the Broadband Gateway on page 148

send-accounting-on

Syntax	<code>send-accounting-on;</code>
Hierarchy Level	[edit unified-edge aaa mobile-profiles <i>map-name</i> radius accounting]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure different services PICs to send the accounting on the RADIUS message to the accounting network element on initialization. If this attribute is not configured, the accounting on the message is not sent by default.
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Overview of AAA on the Broadband Gateway on page 148• accounting on page 588

servers

Syntax `servers server-name {
 address address;
 source-interface interface {
 ipv4-address address;
 }
 accounting-port port-number;
 accounting-secret password;
 allow-dynamic-requests ;
 authentication-port port-number;
 dead-criteria retries retry-number interval seconds;
 dynamic-requests-secret password;
 retry attempts;
 revert-interval time;
 secret password;
 timeout seconds;
 }`

Hierarchy Level [edit access radius]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the RADIUS servers to which RADIUS authentication and accounting requests are sent when user equipment sessions are established.

Options *server-name*—Name of the server.

The remaining statements are explained separately.

Required Privilege Level access—To view this statement in the configuration.
 access-control—To add this statement to the configuration.

Related Documentation

- [Overview of AAA on the Broadband Gateway on page 148](#)
- [radius on page 604](#)

source-interface

Syntax	<code>source-interface <i>interface</i> [ipv4-address <i>address</i>];</code>
Hierarchy Level	<code>[edit access radius servers <i>server-name</i>]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the source interface on the gateway from which the RADIUS requests are sent to the RADIUS server. This is a mandatory statement.
Options	<i>interface</i> —Source interface that sends the RADIUS packets. <i>address</i> —IPv4 address of the RADIUS server.
Required Privilege Level	access —To view this statement in the configuration. access-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Overview of AAA on the Broadband Gateway on page 148• servers on page 610

stop-on-access-deny

Syntax	<code>stop-on-access-deny;</code>
Hierarchy Level	<code>[edit unified-edge aaa mobile-profiles <i>map-name</i> radius accounting]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the gateway to send an accounting stop message when authentication fails for a user.
Required Privilege Level	access —To view this statement in the configuration. access-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Overview of AAA on the Broadband Gateway on page 148• accounting on page 588

stop-on-failure

Syntax	stop-on-failure;
Hierarchy Level	[edit unified-edge aaa mobile-profiles <i>map-name</i> radius accounting]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the gateway to send an accounting stop message when the gateway fails to bring up the user equipment session.
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Overview of AAA on the Broadband Gateway on page 148• accounting on page 588

timeout

Syntax	timeout <i>seconds</i> ;
Hierarchy Level	[edit access radius servers <i>server-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the amount of time that the gateway waits to receive a response from a RADIUS server before retrying the request.
Options	<i>seconds</i> —Amount of time to wait. Range: 1 through 90 seconds Default: 3 seconds
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Overview of AAA on the Broadband Gateway on page 148• servers on page 610

traceoptions

Syntax	<pre> traceoptions { file radius; flag send-detail; flag rcv-detail; flag timeout; flag state; level all; server { server <i>name</i>; } } </pre>
Hierarchy Level	[edit access radius]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Trace options related to RADIUS servers.
Options	<p>file radius— Name of the file to receive the output of the tracing operation. The packets that are transmitted to and received from the RADIUS server are logged to the specified filename.</p> <p>flag send-detail—All the attributes that are included in the RADIUS requests are logged to the specified file.</p> <p>flag rcv-detail—All the attributes that are included in the RADIUS response are logged to the file.</p> <p>flag timeout—Set this flag to log events related to response timeouts.</p> <p>flag state—Set this flag to trace the RADIUS server state changes.</p> <p>level all—Various levels of information that can be logged, for example—debug, info, warning, and critical.</p> <p>server—Server to be traced.</p>
Required Privilege Level	<p>access—To view this statement in the configuration.</p> <p>access-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Overview of AAA on the Broadband Gateway on page 148 • radius on page 604

traceoptions

Syntax	<pre>traceoptions { file <i>filename</i>; level all; flag (init config general request response high-availability all); }</pre>
Hierarchy Level	[edit unified-edge aaa]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Define tracing operations for the AAA configuration.
Options	<p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. The packets that are transmitted to and received from the RADIUS server are logged to the specified filename.</p> <p>level all—Various levels of information that can be logged, for example, debug, info, warning, and critical.</p> <p>flag init—Trace initialization-related events.</p> <p>flag config—Trace config-related events.</p> <p>flag general—Trace general events.</p> <p>flag request—Trace request-related events.</p> <p>flag response—Trace response-related events.</p> <p>flag high-availability—Trace high-availability-related events.</p> <p>flag all—Trace all the flag-related events.</p>
Required Privilege Level	<p>access—To view this statement in the configuration.</p> <p>access-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Overview of AAA on the Broadband Gateway on page 148• aaa on page 586

trigger

Syntax	<pre>trigger { no-cos-change; no-deferred-ipv4-address-update; no-ms-timezone-change; no-plmn-change; no-rat-change; no-sgw-change; no-user-location-information-change; }</pre>
Hierarchy Level	[edit unified-edge aaa mobile-profiles <i>map-name</i> radius accounting]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the conditions under which the interim accounting records are sent to the accounting servers. By default, the broadband gateway sends the interim accounting records when various trigger conditions are met.</p> <p>If you want to suppress the gateway from sending the interim accounting records for certain trigger conditions, such trigger condition can be specified in the trigger statement. If you want to have the gateway send periodic interim accounting records, configure interim-interval statement. By default, all these triggers are enabled. To skip generating the interim accounting record, configure the appropriate statement. To generate periodic interim updates, you must configure interim-interval statement.</p>
Options	<p>interim-interval <i>minutes</i>—Set the gateway not to send the interim updates at the specified interval. If you do not set this option, periodic sent updates are not sent.</p> <p>no-cos-change—Set the gateway not to send the accounting-interim update on a CoS change. If you do not set this option, the accounting-interim update is sent on a CoS change.</p> <p>no-deferred-ipv4-address-update—Set the gateway not to send the accounting-interim update on a deferred IPv4 address update. If you do not set this option, the accounting-interim update is sent on a deferred IPv4 address update.</p> <p>no-ms-timezone-change—Set the gateway not to send the accounting-interim update on an MS-Timezone change. If you do not set this option, the accounting-interim update is sent on an MS-Timezone change.</p> <p>no-plmn-change—Set the gateway not to send the accounting-interim update on a PLMN change. If you do not set this option, the accounting-interim update is sent on a PLMN change.</p> <p>no-rat-change—Set the gateway not to send the accounting-interim update on a RAT change. If you do not set this option, the accounting-interim update is sent on a RAT change.</p>

no-sgw-change—Set the gateway not to send the accounting-interim update on an S-GW change. If you do not set this option, the accounting-interim update is sent on an S-GW change.

no-user-location-information-change—Set the gateway not to send the accounting-interim update on a User Location Information change. If you do not set this option, the accounting-interim update is sent on a User Location Information change

Required Privilege Level	access—To view this statement in the configuration.
	access-control—To add this statement to the configuration.
Related Documentation	• Overview of AAA on the Broadband Gateway on page 148
	• accounting on page 588

CHAPTER 19

Address Assignment and DHCP Configuration Statements

- [Address Assignment Configuration Statements on page 618](#)
- [DHCP Configuration Statements on page 629](#)

Address Assignment Configuration Statements

address-assignment (MobileNext Broadband Gateway)

```
Syntax address-assignment {
    mobile-pool-groups {
        group-name {
            [pool-name];
        }
    }
    mobile-pools {
        name {
            ageing-window ageing-window;
            default-pool;
            family (inet | inet6) {
                network {
                    [network-prefix] {
                        external-assigned;
                        range {
                            [name] {
                                external-assigned;
                                high high;
                                low low;
                            }
                        }
                    }
                }
            }
        }
        pool-prefetch-threshold pool-prefetch-threshold;
        pool-snmpt-trap-threshold pool-snmpt-trap-threshold;
        service-mode service-mode-options;
    }
}
```

Hierarchy Level [edit access],
[edit routing-instances *instance-name* access]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the mobile pools and mobile pool groups that are used by the broadband gateway to assign addresses to subscribers. You can configure both IPv4 and IPv6 mobile pools and mobile pool groups.

The remaining statements are explained separately.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation

- [Example: Simple Unified Edge Configuration on page 471](#)

ageing-window (Mobile Pools)

Syntax	<code>ageing-window <i>ageing-window</i>;</code>
Hierarchy Level	[edit access address-assignment mobile-pools <i>name</i>], [edit routing-instances <i>instance-name</i> access address-assignment mobile-pools <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the time up to which IP addresses from the configured mobile pools should not be reused. Addresses from deleted packet data protocol (PDP) contexts or bearers are not reused by the broadband gateway until the time specified.
Default	If you do not configure a value, then the default is used.
Options	<i>ageing-window</i> —Time, in seconds, up to which addresses should not be reused. Range: 1 through 65,535 seconds Default: 2 seconds
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • mobile-pools on page 623

default-pool (Mobile Pools)

Syntax	<code>default-pool;</code>
Hierarchy Level	[edit access address-assignment mobile-pools <i>name</i>], [edit routing-instances <i>instance-name</i> access address-assignment mobile-pools <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the mobile pool as 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).
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • address-assignment (APN) on page 680 • mobile-pools on page 623

external-assigned (Mobile Pools)

Syntax	external-assigned;
Hierarchy Level	<pre>[edit access address-assignment mobile-pools <i>name</i> family inet network <i>network-prefix</i>], [edit access address-assignment mobile-pools <i>name</i> family inet6 network <i>network-prefix</i>], [edit access address-assignment mobile-pools <i>name</i> family inet network <i>network-prefix</i> range <i>name</i>], [edit access address-assignment mobile-pools <i>name</i> family inet6 network <i>network-prefix</i> range <i>name</i>], [edit routing-instances <i>instance-name</i> access address-assignment mobile-pools <i>name</i> family inet network <i>network-prefix</i>], [edit routing-instances <i>instance-name</i> access address-assignment mobile-pools <i>name</i> family inet6 network <i>network-prefix</i>], [edit routing-instances <i>instance-name</i> access address-assignment mobile-pools <i>name</i> family inet network <i>network-prefix</i> range <i>name</i>], [edit routing-instances <i>instance-name</i> access address-assignment mobile-pools <i>name</i> family inet6 network <i>network-prefix</i> range <i>name</i>]</pre>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify that the addresses in the associated network prefix or range are assigned by an external authority—for example, by the authentication, authorization, and accounting (AAA) server or statically by the user equipment. You can specify this either for the network prefix or for a range under the network prefix.
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• network (Mobile Pools) on page 624• range (Mobile Pools) on page 627

family (Mobile Pools)

```
Syntax  family (inet | inet6) {
        network {
            [network-prefix] {
                external-assigned;
                range {
                    [name] {
                        external-assigned;
                        high high;
                        low low;
                    }
                }
            }
        }
    }
```

Hierarchy Level [edit access address-assignment mobile-pools *name*],
[edit routing-instances *instance-name* access address-assignment mobile-pools *name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the protocol family information for the mobile pool. Mobile pools must have either **inet** (IPv4) or **inet6** (IPv6) configured.



NOTE: A mobile pool can have either **inet** (IPv4) or **inet6** (IPv6) configured but not both.

Options **inet**—IP version 4 (IPv4).


inet6—IP version 6 (IPv6).

The remaining statements are explained separately.

Required Privilege Level **access**—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation • [mobile-pools on page 623](#)

mobile-pool-groups

Syntax	<pre>mobile-pool-groups { group-name { [pool-name]; } }</pre>
Hierarchy Level	[edit access address-assignment], [edit routing-instances <i>instance-name</i> access address-assignment]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the mobile pool groups that are used by the broadband gateway to assign addresses to subscribers. You can configure both IPv4 and IPv6 pool groups.</p> <p>Mobile pool groups are a collection of one or more mobile pools. 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.</p>
Options	<p>group-name—Name of the mobile pool group. Range: Up to 63 characters</p> <p>pool-name—Name of the mobile pool. To specify multiple mobile pools, include the pool-name statement multiple times. Range: Up to 63 characters</p>
	<div><p>NOTE: The mobile pool that you specify must be previously configured on the broadband gateway in the same routing instance as the mobile pool group.</p></div>
	<p>The remaining statements are explained separately.</p>
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• address-assignment (MobileNext Broadband Gateway) on page 618• mobile-pools on page 623

mobile-pools

```
Syntax  mobile-pools {
        name {
            ageing-window ageing-window;
            default-pool;
            family (inet | inet6) {
                network {
                    [network-prefix] {
                        external-assigned;
                        range {
                            [name] {
                                external-assigned;
                                high high;
                                low low;
                            }
                        }
                    }
                }
            }
        }
        pool-prefetch-threshold pool-prefetch-threshold;
        pool-snmp-trap-threshold pool-snmp-trap-threshold;
        service-mode service-mode-options;
    }
```

Hierarchy Level [edit access address-assignment],
[edit routing-instances *instance-name* access address-assignment]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the mobile pools that are used by the broadband gateway to assign addresses to subscribers. You can configure both IPv4 and IPv6 mobile pools and various other parameters related to address assignment.

Options *name*—Name of the mobile pool.


Range: Up to 63 characters

The remaining statements are explained separately.

Required Privilege Level access—To view this statement in the configuration.
access-control—To add this statement to the configuration.

Related Documentation • [address-assignment \(MobileNext Broadband Gateway\) on page 618](#)

network (Mobile Pools)

Syntax	<pre>network { [network-prefix] { external-assigned; range { [name] { external-assigned; high high; low low; } } } }</pre>
Hierarchy Level	[edit access address-assignment mobile-pools <i>name</i> family inet], [edit access address-assignment mobile-pools <i>name</i> family inet6], [edit routing-instances <i>instance-name</i> access address-assignment mobile-pools <i>name</i> family inet], [edit routing-instances <i>instance-name</i> access address-assignment mobile-pools <i>name</i> family inet6]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the network prefix for the mobile pool for IPv4 or IPv6 addresses. The broadband gateway uses the network prefix to assign IP addresses to mobile subscribers. In addition, if an address range is configured under the network prefix, then addresses are allocated only from the specified range.
	<div> NOTE: At least one network prefix must be configured.</div>
Options	network-prefix —Network prefix (IPv4 or IPv6). The remaining statements are explained separately.
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• range (Mobile Pools) on page 627


pool-prefetch-threshold (Mobile Pools)

Syntax	<code>pool-prefetch-threshold <i>pool-prefetch-threshold</i>;</code>
Hierarchy Level	[edit access address-assignment mobile-pools <i>name</i>], [edit routing-instances <i>instance-name</i> access address-assignment mobile-pools <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the pool usage threshold in the mobile pool for pre-fetching addresses. The pre-fetch threshold is used when the pool is configured with prefixes, and when prefixes are added to an existing pool.
Default	If you do not configure a value, then the default is used.
Options	<i>pool-prefetch-threshold</i> —Pre-fetch threshold percentage. Range: 1 through 100 Default: 80
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• mobile-pools on page 623

pool-snmpt-trap-threshold (Mobile Pools)

Syntax	<code>pool-snmpt-trap-threshold <i>pool-snmpt-trap-threshold</i>;</code>
Hierarchy Level	[edit access address-assignment mobile-pools <i>name</i>], [edit routing-instances <i>instance-name</i> access address-assignment mobile-pools <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	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.
Default	If you do not configure a value, then the default is used.
Options	<i>pool-snmpt-trap-threshold</i> —Threshold percentage. Range: 1 through 100 Default: 80
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• mobile-pools on page 623

range (Mobile Pools)

Syntax	<pre>range { [name] { external-assigned; high high; low low; } }</pre>
Hierarchy Level	<pre>[edit access address-assignment mobile-pools name family inet network network-prefix], [edit access address-assignment mobile-pools name family inet6 network network-prefix], [edit routing-instances instance-name access address-assignment mobile-pools name family inet network network-prefix], [edit routing-instances instance-name access address-assignment mobile-pools name family inet6 network network-prefix]</pre>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the address ranges within the network prefix of the mobile pool. This configuration is optional. If a range is specified, then the broadband gateway assigns addresses only from the specified range.
Options	<p>high high—Upper address (IPv4) or prefix (IPv6) of the range.</p> <p>low low—Lower address (IPv4) or prefix (IPv6) of the range.</p>
	<div>  <p>NOTE: If you specify a range, then the high and low statements are mandatory.</p> </div>
	<p>name—Name of the address range.</p> <p>Range: Up to 63 characters</p> <p>Syntax: The name must be unique within a mobile pool.</p> <p>The remaining statement is explained separately.</p>
Required Privilege Level	<p>access—To view this statement in the configuration.</p> <p>access-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> network (Mobile Pools) on page 624

service-mode (Mobile Pools)

Syntax	<code>service-mode <i>service-mode-options</i>;</code>
Hierarchy Level	[edit access address-assignment mobile-pools <i>name</i>], [edit routing-instances <i>instance-name</i> access address-assignment mobile-pools <i>name</i>]
Description	<p>Specify that the mobile pool should be in maintenance mode. You do this if you want to carry out maintenance tasks like deleting or modifying a mobile pool and so on. See the <i>Maintenance Mode</i> chapter in the <i>MobileNext Broadband Gateway Configuration Guide</i> for a list of the maintenance tasks that can be carried out when the mobile pool is in maintenance mode.</p> <p>When in the Maintenance Mode Active Phase, all the valid attributes on the object can be modified. In other cases, only the non-maintenance mode attributes can be modified.</p>
Options	<i>service-mode-options</i> —Specify the service mode. Currently, maintenance mode is the only option supported.
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Changing Address Attributes in the Mobile Address Pool on page 408• Deleting a Mobile Address Pool on page 410• mobile-pools on page 623

DHCP Configuration Statements

bind-interface

Syntax	<code>bind-interface <i>interface-name</i> [<i>ip-address</i>];</code>
Hierarchy Level	<code>[edit routing-instances <i>name</i> system services dhcp-proxy-client dhcpv4-profiles <i>name</i>]</code> <code>[edit routing-instances <i>name</i> system services dhcp-proxy-client dhcpv6-profiles <i>name</i>]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the interface on which the DHCP proxy client communicates with servers. For the DHCPv4 proxy client, the interface must be configured with the valid inet address and inet address family. Similarly, for DHCPv6, the interface must be configured with the valid inet6 address and inet6 family.
Example 1: Configuring dhcp-proxy-client with interfaces.	<pre> ge-0/1/5 { description "Interface facing DHCP server side"; unit 0 { family inet { address 10.1.1.1/24; } } } </pre>
Example 2: Configuring dhcp-proxy-client v4 profile	<pre> services { dhcp-proxy-client { dhcpv4-profiles dhcp-prof-1 { bind-interface ge-0/1/5.0; servers 10.1.1.2; } } } </pre>
Options	<i>interface-name</i> —Bind interface.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • DHCP Overview on page 207 • dhcp-proxy-client on page 632

dead-server-retry-interval

Syntax	<code>dead-server-retry-interval <i>n seconds</i>;</code>
Hierarchy Level	[edit routing-instances <i>name</i> system services dhcp-proxy-client dhcpv4-profiles <i>name</i>] [edit routing-instances <i>name</i> system services dhcp-proxy-client dhcpv6-profiles <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the number of seconds before the broadband gateway reconnects with a dead server, which was marked down in previous attempts. A server is marked down if there is no response for multiple attempts. The count for the number of attempts is gathered from dead-server-successive-retry-attempt .
Default	If you do not include this statement, the time interval is set to 300 seconds.
Options	<i>n seconds</i> —Time interval, in seconds, between retries. Range: 300 through 3600 seconds.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• DHCP Overview on page 207• dhcp-proxy-client on page 632

dead-server-successive-retry-attempt

Syntax	<code>dead-server-successive-retry-attempt <i>number-of-attempts</i>;</code>
Hierarchy Level	[edit routing-instances <i>name</i> system services dhcp-proxy-client dhcpv4-profiles <i>name</i>] [edit routing-instances <i>name</i> system services dhcp-proxy-client dhcpv6-profiles <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the number of successive retry attempts before declaring an unresponsive server dead. The retry attempts are specified as a count through this configuration. If a server is marked dead, no DHCP packets are sent to the server until the dead timer expires and the server comes alive. The dead timer is started with the timeout specified using the dead-server-retry-interval statement.
Default	If you do not include this statement, the default value is used.
Options	count —Number of attempts between retries. Range: 5 through 1000 Default: 5
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • DHCP Overview on page 207 • dhcp-proxy-client on page 632

dhcp-proxy-client

```
Syntax  dhcp-proxy-client {
        dhcpv4-profiles {
            dhcpv4-client-profile-name-1 {
                bind-interface interface-name [ip-address];
                dead-server-retry-interval n seconds;
                dead-server-successive-retry-attempt number-of-attempts;
                dhcp-server-selection-algorithm (highest-priority-server | round-robin);
                lease-time n seconds;
                pool-name strings;
                retransmission-attempt number-of-attempts;
                retransmission-interval n seconds;
                server {
                    ipv4-address priority value;
                }
            }
        }
        dhcpv6-profiles {
            dhcpv6-client-profile-name-1 {
                bind-interface interface-name [ip-address];
                dead-server-retry-interval n seconds;
                dead-server-successive-retry-attempt number-of-attempts;
                dhcp-server-selection-algorithm (highest-priority-server | round-robin);
                lease-time n seconds;
                pool-name strings;
                retransmission-attempt number-of-attempts;
                retransmission-interval n seconds;
                server {
                    ipv6-address priority value;
                }
            }
        }
        trace-options {
            file;
            flag;
        }
    }
```

Hierarchy Level [edit routing-instances *name* system services]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the Dynamic Host Configuration Protocol (DHCP) proxy client parameters to enable DHCP-based IPv4 or IPv6 address allocation for mobile users. The DHCP proxy client acquires a subnet (IPv4) and prefix (IPv6) from the server as per DHCP IETF specifications. After the subnet or prefix is obtained from the server, the DHCP proxy client is managed locally for the mobile subscriber. When all mobile subscribers are detached from GGSN or P-GW, the acquired subnet or prefix is released and the DHCP server can be assigned to some other GGSN or P-GW.

Options The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [DHCP Overview on page 207](#)
- [services on page 641](#)

dhcp-server-selection-algorithm

Syntax dhcp-server-selection-algorithm (highest-priority-server | round-robin);

Hierarchy Level [edit routing-instances *name* system services dhcp-proxy-client dhcpv4-profiles *name*]
[edit routing-instances *name* system services dhcp-proxy-client dhcpv6-profiles *name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the algorithm used to select DHCP servers with which to communicate when multiple servers are configured. The DHCP server is selected either by the highest priority or by round-robin method, according to the option specified for server selection.

Default If you do not include this statement, the default selection is set to **round-robin**.

Options *round-robin*—Algorithm in which the selection is activated in a fixed cyclic order.
highest-priority-server—Most suitable algorithm is selected.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [DHCP Overview on page 207](#)
- [dhcp-proxy-client on page 632](#)

dhcpv4-profiles

Syntax	<pre>dhcpv4-profiles <i>profile-name</i> { <i>bind-interface interface-name</i> [<i>ip-address</i>]; <i>dead-server-retry-interval n seconds</i>; <i>dead-server-successive-retry-attempt number-of-attempts</i>; <i>dhcp-server-selection-algorithm</i> (highest-priority-server round-robin); <i>lease-time n seconds</i>; <i>pool-name strings</i>; <i>retransmission-attempt number-of-attempts</i>; <i>retransmission-interval n seconds</i>; server { <i>ipv4-address priorityvalue</i>; } }</pre>
Hierarchy Level	[edit routing-instances <i>name</i> system dhcp-proxy-client]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure DHCPv4 proxy client profiles. The APN refers to the DHCP profiles to obtain the subnet from the DHCP server. Multiple APNs can refer to the same DHCP profile or a single DHCP profile.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• DHCP Overview on page 207• dhcp-proxy-client on page 632

dhcipv6-profiles

Syntax	<pre>dhcipv6-profiles <i>profile-name</i> { bind-interface <i>interface-name</i> [<i>ip-address</i>]; dead-server-retry-interval <i>n seconds</i>; dead-server-successive-retry-attempt <i>number-of-attempts</i>; dhcp-server-selection-algorithm (<i>highest-priority-server</i> <i>round-robin</i>); lease-time <i>n seconds</i>; pool-name <i>strings</i>; retransmission-attempt <i>number-of-attempts</i>; retransmission-interval <i>n seconds</i>; server { <i>ipv6-address</i> <i>priority value</i>; } }</pre>
Hierarchy Level	[edit routing-instances <i>name</i> system dhcp-proxy-client]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure DHCPv6 proxy client profiles. The APN refers to the DHCP profiles to obtain the subnet from the DHCP server. Multiple APNs can refer to the same DHCP profile or a single DHCP profile.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • DHCP Overview on page 207 • dhcp-proxy-client on page 632

lease-time

Syntax	<code>lease-time <i>n seconds</i>;</code>
Hierarchy Level	[edit routing-instances <i>name</i> system services dhcp-proxy-client dhcpv4-profiles <i>name</i>] [edit routing-instances <i>name</i> system services dhcp-proxy-client dhcpv6-profiles <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the minimum and maximum allowable lease times that are accepted in responses from DHCP servers. The default lease time is always in seconds. If the DHCP client does not get the lease time from the DHCP server, it uses the default lease time as the lease time.
Options	<i>seconds</i> —Number of seconds the lease can be held. Range: 60 through 1000
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• DHCP Overview on page 207• dhcp-proxy-client on page 632

pool-name

Syntax	<code>pool-name <i>string</i>;</code>
Hierarchy Level	[edit routing-instances <i>name</i> system services dhcp-proxy-client dhcpv4-profiles <i>name</i>] [edit routing-instances <i>name</i> system services dhcp-proxy-client dhcpv6-profiles <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure a name for the DHCP server address pool. By creating a pool, you can operate in DHCP pool configuration mode. This pool name is sent to the server in subnet-name-suboption of subnet-allocation-option . The pool name is sent only if it is configured and is optional.
Options	<i>pool-name</i> —Name of the pool.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• DHCP Overview on page 207• dhcp-proxy-client on page 632

priority

Syntax	ipv4-address> priority <i>value</i> ; <ipv6-address> priority <i>value</i> ;
Hierarchy Level	[edit routing-instances <i>name</i> system services dhcp-proxy-client dhcpv4-profiles <i>name</i> servers <i>address</i>] [edit routing-instances <i>name</i> system services dhcp-proxy-client dhcpv6-profiles <i>name</i> servers <i>address</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the DHCP server priority. priority is used for selecting a DHCP server through a DHCP discover message. High-priority servers are selected first until the discovered servers are alive and not marked dead. Priority with a lower value is given the highest preference in the process of discovering a server. For example, priority 1 is selected over priority 2 .
Default	If you do not configure this statement, the default priority is used.
Options	value —The router's priority for becoming the designated router. A priority value of 1 means that the router has the least chance of becoming a designated router. Range: 1 through 255 Default: 128
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • DHCP Overview on page 207 • dhcp-proxy-client on page 632

retransmission-attempt

Syntax	retransmission-attempt <i>number-of-attempts</i> ;
Hierarchy Level	[edit routing-instances <i>name</i> system services dhcp-proxy-client dhcpv4-profiles <i>name</i>] [edit routing-instances <i>name</i> system services dhcp-proxy-client dhcpv6-profiles <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the maximum number of times that the system attempts to communicate with the unresponsive DHCP server before it is considered a failure and also the number of attempts to retransmit the DHCP client protocol message.
Default	If you do not configure this statement, the default is used.
Options	<i>number</i> —Number of attempts to retransmit the packet. Range: 0 through 1000 Default: 4
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• DHCP Overview on page 207• dhcp-proxy-client on page 632

retransmission-interval

Syntax	<code>retransmission-interval <i>n seconds</i>;</code>
Hierarchy Level	[edit routing-instances <i>name</i> system services dhcp-proxy-client dhcpv4-profiles <i>name</i>] [edit routing-instances <i>name</i> system services dhcp-proxy-client dhcpv6-profiles <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the amount of time that must pass with no response before the system reattempts to communicate with the DHCP server and the number of seconds between successive retransmissions of DHCP client protocols messages.
Default	If you do not include this statement, the default is used.
Options	<i>n seconds</i> —Number of seconds between successive retransmissions. Range: 4 through 64 Default: 4
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• DHCP Overview on page 207• dhcp-proxy-client on page 632

server

Syntax	<pre>servers { ipv4-address priority value; }</pre>
Hierarchy Level	[edit routing-instances <i>name</i> system services dhcp-proxy-client dhcpv4-profiles <i>name</i>] [edit routing-instances <i>name</i> system services dhcp-proxy-client dhcpv6-profiles <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the list of DHCP servers with which the DHCP proxy clients communicate to obtain IPv4 subnet or IPv6 prefix, which is allocated to mobile users locally in the P-GW/GGSN gateway. This is applicable only to a DHCPv4 profile and a minimum of one server must be configured for effective communication between DHCP proxy clients and the DHCP server.
Options	<p>IPv4—IPv4 address for the server.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• DHCP Overview on page 207• dhcp-proxy-client on page 632

services

```
Syntax  services {
    dhcp-proxy-client {
    dhcpv4-profiles profile-name {
        bind-interface interface-name ip-address;
        dead-server-retry-interval n seconds;
        dead-server-successive-retry-attempt number-of-attempts;
        dhcp-server-selection-algorithm (highest-priority-server | round-robin);
        lease-time n seconds;
        pool-name strings;
        retransmission-attempt number-of-attempts;
        retransmission-interval n seconds;
        server {
            ipv4-address priority value;
        }
    }
    }
    dhcpv6-profiles profile-name {
        bind-interface interface-name ip-address;
        dead-server-retry-interval n seconds;
        dead-server-successive-retry-attempt number-of-attempts;
        dhcp-server-selection-algorithm (highest-priority-server | round-robin);
        lease-time n seconds;
        pool-name strings;
        retransmission-attempt n times;
        retransmission-interval n seconds;
        server {
            ipv6-address priority value;
        }
    }
    }
    trace-options {
        file;
        flag;
    }
}
```

Hierarchy Level [edit routing-instances *name* system]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure to display information about a specific DHCP service.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [DHCP Overview on page 207](#)
- [system on page 642](#)

system

```
Syntax  system {
        services {
            dhcp-proxy-client {
            dhcpv4-profiles profile-name {
                bind-interface interface-name ip-address;
                dead-server-retry-interval n seconds;
                dead-server-successive-retry-attempt number-of-attempts;
                dhcp-server-selection-algorithm (highest-priority-server | round-robin);
                lease-time n seconds;
                pool-name strings;
                retransmission-attempt number-of-attempts;
                retransmission-interval n seconds;
                server {
                    ipv4-address priority value;
                }
            }
        }
        dhcpv6-profiles profile-name {
            bind-interface interface-name ip-address;
            dead-server-retry-interval n seconds;
            dead-server-successive-retry-attempt number-of-attempts;
            dhcp-server-selection-algorithm (highest-priority-server | round-robin);
            lease-time n seconds;
            pool-name strings;
            retransmission-attempt number-of-attempts;
            retransmission-interval n seconds;
            server {
                ipv6-address priority value;
            }
        }
        trace-options {
            file;
            flag;
        }
    }
```

Hierarchy Level [edit routing-instances]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the system parameters.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [DHCP Overview on page 207](#)

trace-options

Syntax	<pre>trace-options { file <i>file</i>; flag <i>flag</i>; }</pre>
Hierarchy Level	[edit routing-instances <i>name</i> system services dhcp-proxy-client]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Define global tracing operations for DHCP proxy client.
Options	<p><i>file</i>—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the /var/log directory.</p> <p><i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• DHCP Overview on page 207• dhcp-proxy-client on page 632

Anchor Packet Forwarding Engine Redundancy and Aggregated Multiservices High Availability Configuration Statements

anchor-pfes

Syntax	<pre>anchor-pfes { [interface <i>interface-name</i>]; }</pre>
Hierarchy Level	<pre>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> system], [edit unified-edge gateways sgw <i>gateway-name</i> system]</pre>
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W.</p> <p>Support at the [edit unified-edge gateways sgw <i>gateway-name</i> system] hierarchy level introduced in Junos OS Mobility Release 11.4W.</p>
Description	<p>Specify the interfaces used for anchoring subscribers in the Packet Forwarding Engine in the broadband gateway.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • system on page 673

anchor-service-pics

Syntax	<pre>anchor-service-pics { [interface <i>interface-name</i>]; }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> system]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	<p>Specify the interfaces used for anchoring mobile subscriber-aware services in the broadband gateway.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• system on page 673


anchor-spics

Syntax	<pre>anchor-spics { [interface <i>interface-name</i>]; }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> system], [edit unified-edge gateways sgw <i>gateway-name</i> system]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> system] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Specify the interfaces used for the mobile control plane in the broadband gateway.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• system on page 673

anchoring-options (Aggregated Packet Forwarding Engine)

Syntax	<pre> anchoring-options { apfe-group-set apfe-group-set; primary-list { [anchoring-device-name]; } secondary anchoring-device-name; warm-standby; } </pre>
Hierarchy Level	[edit interfaces <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the options for the anchor Packet Forwarding Engine redundancy. The redundancy options are configured at the level of the Flexible PIC Concentrator (FPC). The FPCs that are configured for redundancy must be of the same type—that is, they must have the same number of Packet Forwarding Engines and the same forwarding capabilities.</p> <p>The type of redundancy supported is many-to-one (N:1), which means that one Packet Forwarding Engine acts as the backup for one or more (N) Packet Forwarding Engines. When you configure FPCs for anchor Packet Forwarding Engine redundancy, the corresponding anchor Packet Forwarding Engines in each FPC are configured for N:1 redundancy. The first Packet Forwarding Engine of each primary FPC is backed up by the first Packet Forwarding Engine of the backup FPC, the second Packet Forwarding Engine of each primary FPC is backed up by the second Packet Forwarding Engine of the backup FPC, and so on.</p> <p>For example, consider the case when you configure three FPCs—FPC1, FPC2, and FPC3—for redundancy with FPC1 and FPC2 as primary members, and FPC3 as backup. If each FPC has two Packet Forwarding Engines (PFE0 and PFE1), then FPC1-PFE0 and FPC2-PFE0 are backed up by FPC3-PFE0. Similarly, FPC1-PFE1 and FPC2-PFE1 are backed up by FPC3-PFE1.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Interface Redundancy on page 78 • Configuring Interface DPCs or MPCs for User Mobility Traffic on page 66 • Example: Configuring Broadband Gateway Redundancy on page 82 • interfaces (Aggregated Packet Forwarding Engine) on page 660

apfe-group-set (Aggregated Packet Forwarding Engine)

Syntax	<code>apfe-group-set <i>apfe-group-set</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> anchoring-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Specify that the anchor Packet Forwarding Engines belonging to the FPCs configured for redundancy should belong to an aggregated Packet Forwarding Engine (apfe) group set. When you specify an apfe group set, the FPCs configured on the different apfe interfaces share the same fate.</p> <p>For example, you configure two apfe interfaces: apfe0 and apfe1. This means that if an anchor Packet Forwarding Engine on an FPC in apfe0 switches to the corresponding backup anchor Packet Forwarding Engine on the backup FPC, then the anchor Packet Forwarding Engine on the corresponding FPC in apfe1 also switches to the corresponding backup anchor Packet Forwarding Engine on the backup FPC.</p> <div><p>NOTE: The apfe-group-set is configured at the apfe level. Since the apfe interfaces have Packet Forwarding Engine interfaces (pfe-) as their members, the apfe-group-set configuration groups interfaces at the Packet Forwarding Engine level rather than at the FPC level.</p></div>
Default	If you do not configure the apfe-group-set statement, then the apfe interface that you configure behaves as a standalone entity and it is not influenced by other apfe interfaces configured on the broadband gateway.
Options	<p><i>apfe-group-set</i>—Name of the apfe group set.</p> <p>Range: Up to 32 characters</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• anchoring-options (Aggregated Packet Forwarding Engine) on page 647• Configuring Interface Redundancy on page 78• Example: Configuring Broadband Gateway Redundancy on page 82

dedicated (IPsec)

Syntax	<code>dedicated;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>interface-unit-number</i> dial-options]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify that Dynamic End Point (DEP) IP Security (IPsec) tunnels are supported in dedicated logical interface (ifl) mode for the aggregated multiservices (AMS) interface. In dedicated ifl mode, each DEP IPsec tunnel is mapped to one AMS ifl .
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• dial-options (IPsec) on page 649• shared (IPsec) on page 672

dial-options (IPsec)

Syntax	<pre>dial-options { (dedicated shared); ipsec-interface-id <i>ipsec-interface-id</i>; }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>interface-unit-number</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Configure the parameters to support Dynamic End Point (DEP) IP Security (IPsec) tunnels on the aggregated multiservices (AMS) interface. DEP IPsec tunnels are supported in two modes: dedicated logical interface (ifl) mode and shared ifl mode.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• unit (Aggregated Multiservices) on page 674

drop-member-traffic (Aggregated Multiservices)

Syntax	<pre>drop-member-traffic { <i>rejoin-timeout</i> <i>rejoin-timeout</i>; }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> load-balancing-options member-failure-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Specify whether the broadband gateway should drop traffic to a multiservices PIC when it fails.</p> <ul style="list-style-type: none">• For one-to-one (1:1) mobile control plane redundancy, this configuration is valid only when both multiservices PICs have failed.• For many-to-one (N:1) high availability (HA) for service applications (application-level gateway [ALG], Network Address Translation [NAT], and stateful firewall), this configuration is valid only when two or more multiservices PICs have failed. <p>The remaining statement is explained separately.</p>
Default	If this statement is not configured, then the default behavior is to drop member traffic with a rejoin timeout of 120 seconds. If the member does not come back online within this time, then it must be manually brought back into the AMS interface, using the request interface load-balancing revert command.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Session DPC Redundancy on page 76• Example: Configuring Broadband Gateway Redundancy on page 82• member-failure-options (Aggregated Multiservices) on page 665• request interface load-balancing revert (Aggregated Multiservices) on page 1054

enable-rejoin (Aggregated Multiservices)

Syntax	enable-rejoin;
Hierarchy Level	[edit interfaces <i>interface-name</i> load-balancing-options member-failure-options redistribute-all-traffic]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Enable the failed member to rejoin the aggregated multiservices (AMS) interface after the member comes back online.</p> <ul style="list-style-type: none">• For one-to-one (1:1) mobile control plane redundancy, this configuration is used in case both members fail, and it allows the members to rejoin the ams interface automatically.• For many-to-one (N:1) high availability (HA) for service applications (application-level gateway [ALG], Network Address Translation [NAT], and stateful firewall), this configuration allows the failed members to rejoin the pool of active members automatically.
Default	If you do not configure this option, then the failed members do not automatically rejoin the ams interface even after coming back online. For this reason, the inactive member cannot be the backup for the active member (even after it comes back online) unless the request interface load-balancing revert command is explicitly issued to return the inactive member to the active state.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Session DPC Redundancy on page 76• Example: Configuring Broadband Gateway Redundancy on page 82• redistribute-all-traffic (Aggregated Multiservices) on page 670• request interface load-balancing revert (Aggregated Multiservices) on page 1054

family (Aggregated Multiservices)

Syntax	<code>family <i>family</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>interface-unit-number</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure protocol family information for the logical interface.
Options	<i>family</i> —Protocol family. Currently, only one option, inet (IP version 4 suite), is supported.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Session DPC Redundancy on page 76• Example: Configuring Broadband Gateway Redundancy on page 82• unit (Aggregated Multiservices) on page 674

high-availability-options (Aggregated Multiservices)

Syntax high-availability-options {
 many-to-one {
 preferred-backup *preferred-backup*;
 }
 }

Hierarchy Level [edit interfaces *interface-name* load-balancing-options]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the high availability options for the aggregated multiservices (AMS) interface. This configuration is mandatory for mobile control plane redundancy. For service applications, if only the load-balancing feature is being used, then this configuration is optional.

- For one-to-one (1:1) mobile control plane redundancy, the preferred backup multiservices PIC, in hot standby mode, backs up one multiservices PIC.
- For many-to-one (N:1) high availability support for service applications (application-level gateway [ALG], Network Address Translation [NAT], and stateful firewall), the preferred backup multiservices PIC, in hot standby mode, backs up one or more (N) active multiservices PICs.



NOTE: In both cases, if one of the active multiservices PICs goes down, then the backup replaces it as the active multiservices PIC. When the failed PIC comes back up, it becomes the new backup. This is called floating backup.



The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring Session DPC Redundancy on page 76](#)
- [Example: Configuring Broadband Gateway Redundancy on page 82](#)
- [load-balancing-options \(Aggregated Multiservices\) on page 662](#)

interface (Anchor Packet Forwarding Engine)

Syntax	[interface <i>interface-name</i>];
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> system anchor-pfes], [edit unified-edge gateways sgw <i>gateway-name</i> system anchor-pfes]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> system anchor-pfes] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the interface representing the Packet Forwarding Engine used for anchoring subscribers in the broadband gateway. The following conditions are applicable to the anchor Packet Forwarding Engine interfaces configured here:</p> <ul style="list-style-type: none"> The aggregated Packet Forwarding Engine interfaces (apfe) specified in this statement must already be defined at the [edit interfaces] hierarchy level. For a broadband gateway configured as a gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW), the anchor Packet Forwarding Engine interfaces must have mobility ggsn-pgw as their forwarding package at the [edit chassis fpc <i>fpc-slot</i> forwarding-packages] hierarchy level or the [edit chassis fpc <i>fpc-slot</i> pfe <i>pfe-id</i> forwarding-packages] hierarchy level. <p> NOTE: If the specified anchor Packet Forwarding Engine interface is an apfe interface, then all the member interfaces of the apfe interface must have mobility ggsn-pgw as their forwarding package (at the [edit chassis fpc <i>fpc-slot</i> pfe <i>pfe-id</i> forwarding-packages] hierarchy level).</p> <ul style="list-style-type: none"> For a broadband gateway configured as a Serving Gateway (S-GW), the anchor Packet Forwarding Engine interfaces must have mobility sgw as their forwarding package at the [edit chassis fpc <i>fpc-slot</i> forwarding-packages] hierarchy level or the [edit chassis fpc <i>fpc-slot</i> pfe <i>pfe-id</i> forwarding-packages] hierarchy level. <p> NOTE: If the specified anchor Packet Forwarding Engine interface is an apfe interface, then all member interfaces of the apfe interface must have mobility sgw as their forwarding package (at the [edit chassis fpc <i>fpc-slot</i> forwarding-packages] or the [edit chassis fpc <i>fpc-slot</i> pfe <i>pfe-id</i> forwarding-packages] hierarchy levels).</p> <ul style="list-style-type: none"> If an anchor Packet Forwarding Engine interface is a member of an apfe interface, then that anchor interface cannot be specified here. For example, if pfe-2/0/0 is a member interface of apfe interface apfe0, then pfe-2/0/0 cannot be directly specified here.
Options	<i>interface-name</i> —Name of the interface representing the Packet Forwarding Engine.


Syntax: The interface must be a valid Packet Forwarding Engine interface (**apfe** or **pfe-**); for example, **apfe0** or **pfe-1/0/0**.

Required Privilege interface—To view this statement in the configuration.
Level interface-control—To add this statement to the configuration.

Related Documentation

- [anchor-pfes on page 645](#)
- [Configuring Interface Redundancy on page 78](#)
- [Configuring Interface DPCs or MPCs for User Mobility Traffic on page 66](#)
- [Example: Configuring Broadband Gateway Redundancy on page 82](#)
- [show unified-edge ggsn-pgw system interfaces on page 1066](#)
- [show unified-edge sgw system interfaces on page 1068](#)

interface (Services PIC)

Syntax	[interface <i>interface-name</i>];
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> system anchor-service-pics]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the interface representing the services PIC used for anchoring services-related subscriber sessions in the broadband gateway. The following conditions are applicable to the services PIC interfaces configured here:</p> <ul style="list-style-type: none"> • The aggregated multiservices interfaces (ams) specified in this statement must already be defined at the [edit interfaces] hierarchy level. • The services PIC must have the jservices-hcm, jservices-mss, and jservices-crypto-base packages configured at the [edit chassis fpc slot-number pic pic-number adaptive-services service-package extension-provider] hierarchy level. • If a services PIC interface is a member of an aggregated multiservices interface, then that member interface cannot be specified here. For example, if mams-2/0/0 is a member interface of the aggregated multiservices interface ams0, then ms-2/0/0/ cannot be directly specified here.
	<div>  <p>NOTE: If an aggregated multiservices interface (for example ams0) is used for HTTP header enrichment, then load balancing is performed to anchor subscriber-aware services in one of the member interfaces. Otherwise, load balancing is not performed.</p> </div>
Options	<p>interface-name—Name of the interface representing the services PIC.</p> <p>Syntax: The interface must be a valid multiservices interface (ams or ms-a/b/0, where a is the Flexible PIC Concentrator [FPC] slot number and b is the PIC slot number); for example, ams0 or ms-1/0/0.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • anchor-service-pics on page 646 • show unified-edge ggsn-pgw system interfaces on page 1066

interface (Session PIC)

Syntax	<code>[interface <i>interface-name</i>];</code>
Hierarchy Level	<code>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> system anchor-spics]</code> , <code>[edit unified-edge gateways sgw <i>gateway-name</i> system anchor-spics]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the <code>[edit unified-edge gateways sgw <i>gateway-name</i> system anchor-spics]</code> hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the interface representing the session PIC used for the mobile control plane in the broadband gateway. The following conditions are applicable to the session PIC interfaces configured here:</p> <ul style="list-style-type: none"> • The aggregated multiservices interfaces (ams) specified in this statement must already be defined at the <code>[edit interfaces]</code> hierarchy level. • The session PIC must have the jservices-mobile package configured at the <code>[edit chassis fpc <i>slot-number</i> pic <i>pic-number</i> adaptive-services service-package extension-provider]</code> hierarchy level. • If a session PIC interface is a member of an aggregated multiservices interface, then that member interface cannot be specified here. For example, if mams-2/0/0 is a member interface of the aggregated multiservices interface ams0, then ms-2/0/0/ cannot be directly specified here.
Options	<p><i>interface-name</i>—Name of the interface representing the session PIC.</p> <p>Syntax: The interface must be a valid multiservices interface (ams or ms-a/b/0, where a is the Flexible PIC Concentrator [FPC] slot number and b is the PIC slot number); for example, ams0 or ms-1/0/0.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • anchor-spics on page 646 • Configuring Anchor Session DPCs and PFEs on page 71 • show unified-edge ggsn-pgw system interfaces on page 1066 • show unified-edge sgw system interfaces on page 1068

interfaces (Aggregated Multiservices)

```
Syntax  interfaces interface-name {
        load-balancing-options {
            high-availability-options {
                many-to-one {
                    preferred-backup preferred-backup;
                }
            }
            member-failure-options {
                drop-member-traffic {
                    rejoin-timeout rejoin-timeout;
                }
                redistribute-all-traffic {
                    enable-rejoin;
                }
            }
        }
        member-interface interface-name;
    }
    unit interface-unit-number {
        dial-options {
            (dedicated | shared);
            ipsec-interface-id ipsec-interface-id;
        }
        family family;
        load-balancing-options {
            preferred-active interface-name;
        }
    }
}
```

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the aggregated multiservices (AMS) interface. The AMS interface provides the infrastructure for load balancing and high availability (HA).

The high availability feature is used for mobile control plane redundancy and for service applications (application-level gateway [ALG], Network Address Translation [NAT], and stateful firewall). The load-balancing feature is currently used only for service applications. For service applications, load balancing can be used with or without high availability. Mobile control plane load balancing is done by the ingress Packet Forwarding Engine.



NOTE: The interfaces must be valid aggregated multiservices interfaces (ams); for example, ams0 or ams1, and so on. The ams infrastructure is supported only in chassis with Trio-based modules and Multiservices Dense Port Concentrators (MS-DPCs).

The remaining statements are explained separately.

Options	interface-name —Name of the aggregated multiservices interface (ams); for example, ams0 or ams1 , and so on.
Required Privilege Level	interface —To view this statement in the configuration. interface-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Session DPC Redundancy on page 76• Example: Configuring Broadband Gateway Redundancy on page 82

interfaces (Aggregated Packet Forwarding Engine)

Syntax `interfaces interface-name {
 anchoring-options {
 apfe-group-set apfe-group-set;
 primary-list {
 [anchoring-device-name];
 }
 secondary anchoring-device-name;
 warm-standby;
 }
 }`

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the aggregated Packet Forwarding Engine interface (**apfe**) used for anchor Packet Forwarding Engine redundancy on the broadband gateway.

The type of redundancy supported is many-to-one (N:1), which means that one Packet Forwarding Engine acts as the backup for one or more (N) Packet Forwarding Engines. When you configure Flexible PIC Concentrators (FPCs) for anchor Packet Forwarding Engine redundancy, the corresponding anchor Packet Forwarding Engines in each FPC are configured for N:1 redundancy. The first Packet Forwarding Engine of each primary FPC is backed up by the first Packet Forwarding Engine of the backup FPC, the second Packet Forwarding Engine of each primary FPC is backed up by the second Packet Forwarding Engine of the backup FPC, and so on.



NOTE: The interfaces must be valid **apfe** interfaces; for example, **apfe0** or **apfe1**.

The remaining statements are explained separately.

Options **interface-name**—Name of the aggregated Packet Forwarding Engine interface (**ams**); for example, **apfe0** or **apfe1**, and so on.

Required Privilege Level **interface**—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring Interface Redundancy on page 78](#)
- [Example: Configuring Broadband Gateway Redundancy on page 82](#)

ipsec-interface-id (IPsec)

Syntax	<code>ipsec-interface-id <i>ipsec-interface-id</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>interface-unit-number</i> dial-options]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure the IP Security (IPsec) interface identifier for a group of Dynamic End Point (DEP) peers.
Options	<i>ip-sec-interface-id</i> —IPsec interface identifier. Range: 1 through 63 characters
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• dial-options (IPsec) on page 649

load-balancing-options (Aggregated Multiservices)

```
Syntax  load-balancing-options {
        high-availability-options {
            many-to-one {
                preferred-backup preferred-backup;
            }
        }
        member-failure-options {
            drop-member-traffic {
                rejoin-timeout rejoin-timeout;
            }
            redistribute-all-traffic {
                enable-rejoin;
            }
        }
        member-interface interface-name;
    }
```

Hierarchy Level [edit interfaces *interface-name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the high availability (HA) options for the aggregated multiservices (AMS) interface.

The following modes of high availability are supported with AMS:

- One-to-one (1:1) mobile control plane redundancy—In this case, one active multiservices PIC is backed up by one standby multiservices PIC in hot standby mode.
- Many-to-one (N:1) high availability for service applications (application-level gateway [ALG], Network Address Translation [NAT], and stateful firewall)—In this case, one multiservices PIC is the backup (in hot standby mode) for one or more (N) active multiservices PICs. If one of the active multiservices PICs goes down, then the backup replaces it as the active multiservices PIC. When the failed PIC comes back online, it becomes the new backup. This is called floating backup mode.



NOTE: In hot standby mode, the operational state of subscribers anchored on the active multiservices PIC (or PICs) is actively synchronized with the standby multiservices PIC.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring Session DPC Redundancy on page 76](#)
- [Example: Configuring Broadband Gateway Redundancy on page 82](#)

- [interfaces \(Aggregated Multiservices\) on page 658](#)

load-balancing-options (IPsec)

Syntax	<code>load-balancing-options { preferred-active <i>interface-name</i>; }</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>interface-unit-number</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the preferred active member to be used for load balancing the Dynamic End Point (DEP) IP Security (IPsec) tunnels on the aggregated multiservices (AMS) interface. The DEP IPsec tunnels are distributed across the members configured for the AMS interface. However, the active next hop corresponds only to the preferred active member configured here. All other next hops are on standby and no traffic is directed to those members.</p> <p>The remaining statement is explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	• unit (Aggregated Multiservices) on page 674

many-to-one (Aggregated Multiservices)

Syntax	<pre>many-to-one { preferred-backup <i>preferred-backup</i>; }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> load-balancing-options high-availability-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the initial preferred backup for the aggregated multiservices (AMS) interface.



NOTE: The preferred backup must be one of the member interfaces (*mams-*) that have already been configured at the [edit interfaces *interface-name* load-balancing-options] hierarchy level. Even in the case of mobile control plane redundancy, which is one-to-one (1:1), the initial preferred backup is configured at this hierarchy level.

The remaining statements are explained separately.

Options	preferred-backup <i>preferred-backup</i> —Name of the preferred backup member interface. The member interface format is mams-a/b/0 , where a is the Flexible PIC Concentrator (FPC) slot number and b is the PIC slot number.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Session DPC Redundancy on page 76• Example: Configuring Broadband Gateway Redundancy on page 82• high-availability-options (Aggregated Multiservices) on page 653

member-failure-options (Aggregated Multiservices)

Syntax

```
member-failure-options {
  drop-member-traffic {
    rejoin-timeout rejoin-timeout;
  }
  redistribute-all-traffic {
    enable-rejoin;
  }
}
```

Hierarchy Level [edit interfaces *interface-name* load-balancing-options]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the possible behavior for the aggregated multiservices (AMS) interface in case of failure of more than one active member.



NOTE: The `drop-member-traffic` configuration and the `redistribute-all-traffic` configuration are mutually exclusive.

Table 51 on page 665 displays the behavior of the member interface after the failure of the first multiservices PIC. Table 52 on page 666 displays the behavior of the member interface after the failure of two multiservices PICs.



NOTE: The AMS infrastructure has been designed to handle one failure automatically. However, in the unlikely event that more than one multiservices PIC fails, the AMS infrastructure provides configuration options to minimize the impact on existing traffic flows.

Table 51: Behavior of Member Interface After One Multiservices PIC Fails

High Availability Mode	Member Interface Behavior
One-to-one (1:1) mobile control plane redundancy	Automatically handled by the AMS infrastructure
Many-to-one (N:1) high availability support for service applications	Automatically handled by the AMS infrastructure

Table 52: Behavior of Member Interface After Two Multiservices PICs Fail

High Availability Mode	Configuration	rejoin-timeout	Behavior when member rejoins before rejoin-timeout expires	Behavior when member rejoins after rejoin-timeout expires
One-to-one (1:1) mobile control plane redundancy	drop-member-traffic	Configured	<p>The traffic is dropped since both members are down.</p> <p>The first member to rejoin becomes the active member. The second member to rejoin becomes the backup. This behavior is handled automatically by the AMS infrastructure.</p>	<p>The traffic is dropped since both members are down.</p> <p>The first member to rejoin becomes the active member, and the second member to rejoin is moved to the discard state. An explicit request interface load-balancing revert command is required to make the second member rejoin the AMS.</p>
One-to-one (1:1) mobile control plane redundancy	redistribute-all-traffic	Not applicable	<p>The traffic is dropped since both members are down.</p> <p>The first member to rejoin becomes the active member. The second member to rejoin becomes the backup. This behavior is handled automatically by the AMS infrastructure.</p>	
Many-to-one (N:1) high availability support for service applications	drop-member-traffic	Configured	<p>The existing traffic for the second failed member will <i>not</i> be redistributed to the other members.</p> <p>The first member to rejoin becomes an active member. The second member to rejoin becomes the backup. This behavior is handled automatically by the AMS infrastructure.</p>	<p>The existing traffic for the second failed member will <i>not</i> be redistributed to the other members.</p> <p>The first member will rejoin the AMS automatically. However, the other members who are rejoining will be moved to the discard state. An explicit request interface load-balancing revert command is required to make these members rejoin the AMS.</p>
Many-to-one (N:1) high availability support for service applications	redistribute-all-traffic	Not applicable	<p>Before rejoin, the traffic is redistributed to existing active members.</p> <p>After a failed member rejoins, the traffic is load-balanced afresh. This may impact existing traffic flows.</p>	

The remaining statements are explained separately.

Default If **member-failure-options** are not configured, then the default behavior is to drop member traffic with a rejoin timeout of 120 seconds. If the member does not come back online within this time, then it must be manually brought back into the AMS interface, using the **request interface load-balancing revert** command.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

- Related Documentation**
- [Configuring Session DPC Redundancy on page 76](#)
 - [Example: Configuring Broadband Gateway Redundancy on page 82](#)
 - [load-balancing-options \(Aggregated Multiservices\) on page 662](#)
 - [request interface load-balancing revert \(Aggregated Multiservices\) on page 1054](#)

member-interface (Aggregated Multiservices)

Syntax	<code>member-interface <i>interface-name</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> load-balancing-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Specify the member interfaces for the aggregated multiservices (AMS) interface. You can configure multiple interfaces by specifying each interface in a separate statement.</p> <ul style="list-style-type: none"> • For mobile control plane redundancy, which supports one-to-one (1:1) redundancy, you must specify only two interfaces. • For high availability service applications (application-level gateway [ALG], Network Address Translation [NAT], and stateful firewall) that support many-to-one (N:1) redundancy, you can specify two or more interfaces.



NOTE: The member interfaces that you specify must be members of aggregated multiservices interfaces (mams-) on the broadband gateway.



The remaining statements are explained separately.

Options	<i>interface-name</i> —Name of the member interface. The member interface format is mams-a/b/0 , where a is the Flexible PIC Concentrator (FPC) slot number and b is the PIC slot number.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Session DPC Redundancy on page 76 • Example: Configuring Broadband Gateway Redundancy on page 82 • load-balancing-options (Aggregated Multiservices) on page 662

preferred-active (IPsec)

Syntax	<code>preferred-active <i>interface-name</i>;</code>
Hierarchy Level	<code>[edit interfaces <i>interface-name</i> unit <i>interface-unit-number</i> load-balancing-options]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the preferred active member to be used for load balancing the Dynamic End Point (DEP) IP Security (IPsec) tunnels on the aggregated multiservices (AMS) interface. The following conditions are applicable for the preferred active member configured here:</p> <ul style="list-style-type: none">• The preferred active member should already be configured as a member of the AMS interface. (To configure a member interface under AMS, use set member-interface <i>interface-name</i> at the <code>[edit interfaces <i>interface-name</i> load-balancing-options]</code> hierarchy level.)• The preferred active member must not be already configured as the preferred backup for the AMS interface.• If you configure load balancing, then the configuration of the preferred active member is mandatory.
Options	<i>interface-name</i> —Name of the member of AMS interface (mams-); for example, mams-1/0/0 .
Required Privilege Level	interface —To view this statement in the configuration. interface-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• load-balancing-options (IPsec) on page 663

primary-list (Aggregated Packet Forwarding Engine)

Syntax	primary-list { [<i>anchoring-device-name</i>]; }
Hierarchy Level	[edit interfaces <i>interface-name</i> anchoring-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the primary Flexible PIC Concentrators (FPCs) for the anchor Packet Forwarding Engine redundancy.
	 <p>NOTE: You can configure the primary list to contain multiple FPCs. However, all the FPCs must be of the same type—that is, they should have the same number of Packet Forwarding Engines and the same forwarding capabilities.</p>
	To configure multiple primary FPCs, include the anchoring-device-name statement multiple times.
Options	anchoring-device-name —Name of the FPC.
	 <p>NOTE: The interface must be a valid interface (fpc-) that is defined in the broadband gateway interface hierarchy.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • anchoring-options (Aggregated Packet Forwarding Engine) on page 647 • Configuring Interface Redundancy on page 78 • Configuring Interface DPCs or MPCs for User Mobility Traffic on page 66 • Example: Configuring Broadband Gateway Redundancy on page 82

redistribute-all-traffic (Aggregated Multiservices)

Syntax	<code>redistribute-all-traffic { enable-rejoin; }</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> load-balancing-options member-failure-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Enable the option to redistribute traffic of a failed active member to the other active members.</p> <ul style="list-style-type: none">• For one-to-one (1:1) mobile control plane redundancy, since both members have failed, the traffic is dropped.• For many-to-one (N:1) high availability support for Network Address Translation (NAT), the traffic for the failed member is automatically redistributed to the other active members. <p>The remaining statement is explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Session DPC Redundancy on page 76• Example: Configuring Broadband Gateway Redundancy on page 82• member-failure-options (Aggregated Multiservices) on page 665

rejoin-timeout (Aggregated Multiservices)

Syntax	<code>rejoin-timeout <i>rejoin-timeout</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> load-balancing-options member-failure-options drop-member-traffic]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the time by when a failed member should rejoin the aggregated multiservices (AMS) interface automatically. If the failed member does not rejoin by the configured time, then the member is moved to the “inactive” state and the traffic meant for this member is dropped.</p> <p>If the member does not come back online within this time, then it must be manually brought back into the AMS interface, using the request interface load-balancing revert command.</p>
Default	If you do not configure a value, the default value of 120 seconds is used.
Options	<p><i>rejoin-timeout</i>—Time, in seconds, by which a failed member must rejoin.</p> <p>Default: 120 seconds</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Session DPC Redundancy on page 76• drop-member-traffic (Aggregated Multiservices) on page 650• Example: Configuring Broadband Gateway Redundancy on page 82• request interface load-balancing revert (Aggregated Multiservices) on page 1054

secondary (Aggregated Packet Forwarding Engine)

Syntax	<code>secondary <i>anchoring-device-name</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> anchoring-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the secondary Flexible PIC Concentrator (FPC) for the anchor Packet Forwarding Engine redundancy. The Packet Forwarding Engine on the secondary FPC acts as the standby (backup) for the Packet Forwarding Engine on the primary FPCs and takes over as the active Packet Forwarding Engine when a Packet Forwarding Engine on a primary FPC fails.
Options	<i>anchoring-device-name</i> —Name of the FPC.



NOTE: The interface must be a valid interface (*fpc-*) that is defined in the broadband gateway interface hierarchy.

Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• anchoring-options (Aggregated Packet Forwarding Engine) on page 647• Configuring Interface Redundancy on page 78• Example: Configuring Broadband Gateway Redundancy on page 82

shared (IPsec)

Syntax	<code>shared;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>interface-unit-number</i> dial-options]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify that Dynamic End Point (DEP) IP Security (IPsec) tunnels are supported in shared logical interface (ifl) mode for the aggregated multiservices (AMS) interface. In shared ifl mode, one AMS ifl is shared by multiple DEP IPsec tunnels.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• dedicated (IPsec) on page 649• dial-options (IPsec) on page 649

system

Syntax	<pre>system { anchor-pfes { [interface interface-name]; } anchor-service-pics { #P-GW only [interface interface-name]; } anchor-spics { [interface interface-name]; } }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i>], [edit unified-edge gateways sgw <i>gateway-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i>] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Specify the different interfaces used for anchoring subscriber information in the mobile broadband gateway.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• [edit unified-edge gateways] Hierarchy Level on page 563

unit (Aggregated Multiservices)

Syntax `unit interface-unit-number {
 dial-options {
 (dedicated | shared);
 ipsec-interface-id ipsec-interface-id;
 }
 family family;
 load-balancing-options {
 preferred-active interface-name;
 }
 }`

Hierarchy Level [edit interfaces *interface-name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the logical interface on the physical device. You must configure a logical interface to be able to use the physical device.

The remaining statements are explained separately.

Options *interface-unit-number*—Number of the logical unit.



.....
NOTE: Unit 0 is reserved and cannot be configured under the aggregated multiservices interface (ams).
.....


Range: 1 through 16,384

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring Session DPC Redundancy on page 76](#)
- [Example: Configuring Broadband Gateway Redundancy on page 82](#)
- [interfaces \(Aggregated Multiservices\) on page 658](#)

warm-standby (Aggregated Packet Forwarding Engine)

Syntax	warm-standby;
Hierarchy Level	[edit interfaces <i>interface-name</i> anchoring-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the anchor Packet Forwarding Engine redundancy in warm standby mode. In this mode, the secondary Flexible PIC Concentrator (FPC) takes over the role of the primary FPC when a Packet Forwarding Engine on the primary FPC fails. If a Packet Forwarding Engine fails on a primary FPC, then the entire FPC is switched to the secondary FPC.</p> <p>In warm-standby mode, the subscriber sessions are programmed only after the switchover from the primary FPC to the secondary FPC. Based on the subscriber traffic, the programming for some sessions is expedited if needed.</p>
	<div><p>NOTE: When you configure warm standby mode, the switchover from the secondary FPC to the primary FPC takes place at the FPC level.</p></div>
Default	The warm-standby mode is the default.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• anchoring-options (Aggregated Packet Forwarding Engine) on page 647• Configuring Interface Redundancy on page 78• Example: Configuring Broadband Gateway Redundancy on page 82

CHAPTER 21

APN Configuration Statements

- [APN Services Configuration Statements on page 677](#)
- [Service Selection Profiles Configuration Statements on page 754](#)

APN Services Configuration Statements


aaa (APN Address Assignment)

Syntax	<code>aaa;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> address-assignment]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the address assignment option so that the authentication, authorization, and accounting (AAA) server assigns IP addresses for subscribers. If this option is configured, then the broadband gateway uses the IP address returned by the AAA server as part of the subscriber authentication.
Default	If you omit the aaa statement, the default address assignment option is local . This means that the IP addresses are assigned by the broadband gateway using the mobile pool or mobile pool group configured on the access point name (APN). If a pool or a group is not specified, then the default pool is used to assign the IP address. The default mobile pool is configured in the routing instance that is associated with the mobile interface of the APN.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• address-assignment (APN) on page 680• Enabling Address Assignment by the RADIUS Server on page 191• Configuring Address Assignment on a Broadband Gateway APN on page 115

aaa-override (APN Address Assignment)

Syntax	aaa-override;
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> address-assignment dhcp-proxy-client], [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> address-assignment local]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify that the IP address returned by the authentication, authorization, and accounting (AAA) server overrides the address from the subnet returned from the Dynamic Host Configuration Protocol (DHCP) server, or the address obtained from the mobile pool or mobile pool group locally configured on the broadband gateway. If the AAA server provides the address for the user equipment (UE), then the broadband gateway does not assign an address from the subnet, which is returned from the DHCP server for this APN, or the address obtained from the locally configured mobile pool or mobile pool group.
Default	If you do not configure this statement, then the IP address from the subnet returned from the DHCP server, or the address obtained from the mobile pool or mobile pool group locally configured on the broadband gateway, is used depending on the configuration.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring AAA-Assigned Addresses to Override Locally or DHCP-Assigned Addresses on page 191• dhcp-proxy-client (APN Address Assignment) on page 702• local (APN Address Assignment) on page 719

aaa-profile (APN)

Syntax	<code>aaa-profile <i>aaa-profile</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the authentication, authorization, and accounting (AAA) profile to be used for the access point name (APN). The AAA profile is used to authorize whether a default bearer or a primary packet data protocol (PDP) context can be activated for a subscriber. In addition, the AAA profile is also used to pass the subscriber's accounting information to the AAA server.
	<div>  <p>NOTE: The AAA profiles should already be configured on the broadband gateway.</p> </div>
Options	<i>aaa-profile</i> —Name of the AAA profile.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • apns on page 691 • Configuring General APN Parameters on the Broadband Gateway on page 109 • Example: Configuring Broadband Gateway APNs on page 126

address-assignment (APN)

```
Syntax  address-assignment {  
        aaa;  
        allow-static-ip-address {  
            no-address-verify;  
        }  
        dhcp-proxy-client {  
            aaa-override;  
        }  
        dhcpv4-proxy-client-profile {  
            logical-system logical-system;  
            pool-name pool-name;  
            profile-name profile-name;  
            routing-instance routing-instance;  
        }  
        dhcpv6-proxy-client-profile {  
            logical-system logical-system;  
            pool-name pool-name;  
            profile-name profile-name;  
            routing-instance routing-instance;  
        }  
        inet-pool {  
            exclude-pools [value];  
            group group;  
            pool pool;  
        }  
        inet6-pool {  
            exclude-v6pools [value];  
            group group;  
            pool pool;  
        }  
        local {  
            aaa-override;  
        }  
    }
```

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name* apn-services apns *name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the address assignment parameters for an access point name (APN). These parameters are used by the broadband gateway to assign IP addresses to mobile devices.

The following methods of allocating IP addresses are supported by the broadband gateway:

- AAA—IP addresses are allocated by the authentication, authorization, and accounting (AAA) server.
- DHCP—IP addresses are allocated by the broadband gateway using the IP addresses returned by the Dynamic Host Configuration Protocol (DHCP) server. The broadband gateway uses the information configured in the DHCP proxy client profile to access the IP address returned by the DHCP server.

- Local—IP addresses are allocated by the broadband gateway using a local mobile pool or mobile pool group configured on the APN. If a mobile pool or a mobile pool group is not specified, then the default mobile pool is used to assign the IP address. The default pool is configured in the routing instance that is associated with the mobile interface of the APN.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [address-assignment \(MobileNext Broadband Gateway\) on page 618](#)
- [apns on page 691](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 115](#)
- [Example: Configuring Broadband Gateway APNs on page 126](#)

allow-network-behind-mobile

Syntax `allow-network-behind-mobile;`

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name* apn-services apns *name*]

Release Information Statement introduced in Junos OS Mobility Release 11.4W.

Description Specify that support for network behind mobile is allowed for the access point name (APN). The broadband gateway acts as the IP anchor for devices that are behind the user equipment and forwards traffic to and from these devices

Default If you do not configure this statement, then support for network behind mobile is disabled by default.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.


Related Documentation

- [Configuring the Networks Behind the Mobile Equipment Feature on page 131](#)
- [network-behind-mobile on page 725](#)


allow-static-ip-address (APN Address Assignment)

Syntax	<code>allow-static-ip-address { no-address-verify; }</code>
Hierarchy Level	[edit unified-edge gateways <i>ggsn-pgw gateway-name</i> apn-services apns <i>name</i> address-assignment]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>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 Session Request message.</p> <p>The remaining statement is explained separately.</p>
Default	If you omit the allow-static-ip-address statement, then the static IP address provided by the user equipment is not allowed by the broadband gateway.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• address-assignment (APN) on page 680• Configuring Address Assignment on a Broadband Gateway APN on page 115


anchor-pfe-ipv4-nbm-prefixes

Syntax	anchor-pfe-ipv4-nbm-prefixes <i>maximum-ipv4-prefixes</i> ;
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Configure the maximum number of IPv4 prefixes (for devices behind the user equipment) allowed for each anchor Packet Forwarding Engine on the MobileNext Broadband Gateway. This configuration allows you to restrict the memory used for IPv4 prefixes (for network behind mobile) in order to prevent the IPv4 prefixes from using the main route memory of the anchor Packet Forwarding Engine.
<div>  <p>NOTE: Even if you configure the <code>anchor-pfe-ipv4-nbm-prefixes</code> statement, this does not guarantee that the configured number of IPv4 prefixes will be supported. It is possible that the anchor Packet Forwarding Engine will reject the creation of a prefix due to lack of available memory. If sufficient memory is available, then the anchor Packet Forwarding Engine conforms to the number of prefixes configured.</p> </div>	
Options	<p><i>maximum-ipv4-prefixes</i>—Maximum number of IPv4 prefixes, in multiples of thousand, per anchor Packet Forwarding Engine.</p> <p>Range: 16 through 128,000 thousand IPv4 prefixes</p> <p>Default: 64,000 IPv4 prefixes</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring the Networks Behind the Mobile Equipment Feature on page 131 • network-behind-mobile on page 725

anchor-pfe-ipv6-nbm-prefixes

Syntax	anchor-pfe-ipv6-nbm-prefixes <i>maximum-ipv6-prefixes</i> ;
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Configure the maximum number of IPv6 prefixes (for devices behind the user equipment) allowed for each anchor Packet Forwarding Engine on the MobileNext Broadband Gateway. This configuration allows you to restrict the memory used for IPv6 prefixes (for network behind mobile) in order to prevent the IPv6 prefixes from using the main route memory of the anchor Packet Forwarding Engine.
	<div><p>NOTE: Even if you configure the <code>anchor-pfe-ipv6-nbm-prefixes</code> statement, this does not guarantee that the configured number of IPv6 prefixes will be supported. It is possible that the anchor Packet Forwarding Engine will reject the creation of a prefix due to lack of available memory. If sufficient memory is available, then the anchor Packet Forwarding Engine conforms to the number of prefixes configured.</p></div>
Options	<p><i>maximum-ipv6-prefixes</i>—Maximum number of IPv6 prefixes, in multiples of thousand, per anchor Packet Forwarding Engine.</p> <p>Range: 4 through 128,000 IPv6 prefixes</p> <p>Default: 16,000 IPv6 prefixes.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Networks Behind the Mobile Equipment Feature on page 131• network-behind-mobile on page 725

anonymous-user (APN)

Syntax	<pre>anonymous-user { password <i>password</i>; (use-apnname use-imsi use-msisdn user-name <i>username</i>); }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure a default username and password for the non-transparent access point name (APN) to authenticate anonymous users who are setting up sessions on the broadband gateway.</p> <p>When a Create Packet Data Protocol (PDP) Context Request or a Create Session Request message is received for a session without the Protocol Configuration Options (PCO) Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP) information, the anonymous user options configured for the APN are used for user authentication with the authentication, authorization, and accounting (AAA) server.</p> <p>If the PCO PAP or CHAP information is included in the Create PDP Context Request or the Create Session Request message received for a session, then the username and password information is obtained from the PCO PAP or CHAP information. This username and password combination overrides the anonymous user options that you configured.</p> <div style="margin-top: 20px;">  <p>NOTE: The information about the AAA server is obtained from the AAA profile that you specify for the APN.</p> </div>
Options	<p>password <i>password</i>—Password for user authentication. Range: Up to 32 characters</p> <p>use-apnname use-imsi use-msisdn user-name <i>username</i>—Choose the type of username to be used for anonymous users in the APN.</p> <ul style="list-style-type: none"> • use-apnname—Use the APN name as the username to authenticate users. • use-imsi—Use the International Mobile Subscriber Identity (IMSI) of the user's device as the username to authenticate users. • use-msisdn—Use the Mobile Station ISDN (MSISDN) number of the user's device as the username to authenticate users. • <i>username</i>—Default username to be used for authentication.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

- Related Documentation**
- [apns on page 691](#)
 - [Configuring Anonymous Users on a Broadband Gateway APN on page 114](#)

apn-data-type

Syntax	apn-data-type (ipv4 ipv4v6 ipv6);
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the type of addresses (IPv4, IPv6, or both IPv4 and IPv6) that the access point name (APN) can allocate for sessions attaching to the APN.
Default	If you do not specify a value, the default value is ipv4 ; that is, the APN allocates only IPv4 addresses for sessions attaching to that APN.
Options	<p>ipv4—Allocate only IPv4 addresses for sessions attaching to the APN.</p> <p>ipv4v6—Allocate both IPv4 or IPv6 addresses (or only an IPv4 or an IPv6 address) for sessions (based on the request) attaching to the APN.</p> <p>ipv6—Allocate only IPv6 addresses for sessions attaching to the APN.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• apns on page 691• Configuring General APN Parameters on the Broadband Gateway on page 109

apn-services

```

Syntax  apn-services {
        apns {
            [name] {
                aaa-profile aaa-profile;
                address-assignment {
                    aaa;
                    allow-static-ip-address {
                        no-address-verify;
                    }
                    dhcp-proxy-client {
                        aaa-override;
                    }
                    dhcpv4-proxy-client-profile {
                        logical-system logical-system;
                        pool-name pool-name;
                        profile-name profile-name;
                        routing-instance routing-instance;
                    }
                    dhcpv6-proxy-client-profile {
                        logical-system logical-system;
                        pool-name pool-name;
                        profile-name profile-name;
                        routing-instance routing-instance;
                    }
                    inet-pool {
                        exclude-pools [value];
                        group group;
                        pool pool;
                    }
                    inet6-pool {
                        exclude-v6pools [value];
                        group group;
                        pool pool;
                    }
                    local {
                        aaa-override;
                    }
                }
            }
            allow-network-behind-mobile;
            anonymous-user {
                password password;
                (use-apnname | use-imsi | use-msisdn | user-name username);
            }
            apn-data-type (ipv4 | ipv4v6 | ipv6);
            apn-type (real | virtual | virtual-pre-authenticate);
            block-visitors;
            charging {
                default-profile default-profile;
                home-profile home-profile;
                profile-selection-order [profile-selection-method];
                roamer-profile roamer-profile;
                visitor-profile visited-profile;
            }
        }
    }

```

```

}
description description;
dns-server {
    primary-v4 primary-v4;
    primary-v6 primary-v6;
    secondary-v4 secondary-v4;
    secondary-v6 secondary-v6;
}
idle-timeout idle-timeout;
idle-timeout-direction (both | uplink);
inter-mobile-traffic {
    (deny | redirect redirect);
}
local-policy-profile local-policy-profile;
maximum-bearers maximum-bearers;
mobile-interface mobile-interface;
nbns-server {
    primary-v4 primary-v4;
    secondary-v4 secondary-v4;
}
network-behind-mobile {
    imsi imsi {
        prefix-v4 [ipv4-prefix];
        prefix-v6 [ipv6-prefix];
    }
}
p-cscf{
    [address];
}
restriction-value restriction-value;
selection-mode {
    (from-ms | from-sgsn | no-subscribed);
}
service-mode service-mode-options;
service-selection-profile service-selection-profile;
session-timeout session-timeout;
verify-source-address {
    disable;
}
wait-accounting;
}
}
}

```

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description	<p>Configure the access point name (APN) selection function for the broadband gateway. The APN selection function determines whether the broadband gateway is responsible for servicing the subscriber. If the gateway is responsible, then the APN selection function selects the Packet Data Network (PDN) service that is applicable for the subscriber. You can configure different parameters related to the device, network, and subscription to provide an enhanced selection function.</p> <p>The APN selection function determines which APN and service types a Mobile Station (MS) or user equipment (UE) device should use.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• [edit unified-edge gateways ggsn-pgw <gateway-name>] Hierarchy Level on page 564• Configuring APNs on the MobileNext Broadband Gateway Overview on page 105• Example: Configuring Broadband Gateway APNs on page 126

apn-type

Syntax	<code>apn-type (real virtual virtual-pre-authenticate);</code>
Hierarchy Level	<code>[edit unified-edge gateways ggsn-pgw gateway-name apn-services apns name]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Specify the type of access point name (APN). The following APN types are supported:</p> <ul style="list-style-type: none">• real—Configure the APN as real if the APN name sent in the GTP Create message will be used for creating the session.• virtual—Configure the APN as virtual if the APN name sent in the GTP Create message will be mapped to a different (real) APN. The mapped (real) APN is then used to set up the session. A service selection profile must be configured so that the virtual APN can be mapped to a real APN.• virtual-pre-authenticate—Configure the APN as virtual-pre-authenticate if the APN name sent in the GTP Create message will be mapped to a different (real) APN. The mapping in this case is provided by the authentication, authorization, and accounting (AAA) server in the authentication (Access Accept) message. You must configure AAA authentication for this APN so that the virtual APN can be mapped to a real APN.
Default	If you do not specify a value, the default value is real .
Options	<p>real—Specify that the APN is a real APN.</p> <p>virtual—Specify that the APN is a virtual APN.</p> <p>virtual-pre-authenticate—Specify that the APN is a virtual APN that will be mapped to a real APN using AAA authentication.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• apns on page 691• Configuring General APN Parameters on the Broadband Gateway on page 109

apns

```
Syntax  apns {
        [name] {
            aaa-profile aaa-profile;
            address-assignment {
                aaa;
                allow-static-ip-address {
                    no-address-verify;
                }
                dhcp-proxy-client {
                    aaa-override;
                }
                dhcpv4-proxy-client-profile {
                    logical-system logical-system;
                    pool-name pool-name;
                    profile-name profile-name;
                    routing-instance routing-instance;
                }
                dhcpv6-proxy-client-profile {
                    logical-system logical-system;
                    pool-name pool-name;
                    profile-name profile-name;
                    routing-instance routing-instance;
                }
            }
            inet-pool {
                exclude-pools [value];
                group group;
                pool pool;
            }
            inet6-pool {
                exclude-v6pools [value];
                group group;
                pool pool;
            }
            local {
                aaa-override;
            }
        }
        allow-network-behind-mobile;
        anonymous-user {
            password password;
            (use-apnname | use-imsi | use-msisdn | user-name username);
        }
        apn-data-type (ipv4 | ipv4v6 | ipv6);
        apn-type (real | virtual | virtual-pre-authenticate);
        block-visitors;
        charging {
            default-profile default-profile;
            home-profile home-profile;
            profile-selection-order [profile-selection-method];
            roamer-profile roamer-profile;
            visitor-profile visited-profile;
        }
    }
```

```

description description;
dns-server {
    primary-v4 primary-v4;
    primary-v6 primary-v6;
    secondary-v4 secondary-v4;
    secondary-v6 secondary-v6;
}
idle-timeout idle-timeout;
idle-timeout-direction (both | uplink);
inter-mobile-traffic {
    (deny | redirect redirect);
}
local-policy-profile local-policy-profile;
maximum-bearers maximum-bearers;
mobile-interface mobile-interface;
nbns-server {
    primary-v4 primary-v4;
    secondary-v4 secondary-v4;
}
network-behind-mobile {
    imsi imsi {
        prefix-v4 [ipv4-prefix];
        prefix-v6 [ipv6-prefix];
    }
}
p-cscf{
    [address];
}
restriction-value restriction-value;
selection-mode {
    (from-ms | from-sgsn | no-subscribed);
}
service-mode service-mode-options;
service-selection-profile service-selection-profile;
session-timeout session-timeout;
verify-source-address {
    disable;
}
wait-accounting;
}
}

```

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name* apn-services]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the access point name (APN) for the broadband gateway. The APN is a unique identifier used by the broadband gateway to identify each attached IP network, which is called an APN network or a Packet Data Network (PDN). The APN determines authorization and address allocation methods, charging rules, several types of timeouts, and various other parameters that characterize the user session to an IP network.

The remaining statements are explained separately.

Options	<p><i>name</i>—Name of the APN.</p> <p>Range: Up to 100 characters</p> <p>Syntax: Can contain only letters, numbers, decimal points, and dashes</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • apn-services on page 687 • Configuring APNs on the MobileNext Broadband Gateway Overview on page 105 • Configuring General APN Parameters on the Broadband Gateway on page 109 • Example: Configuring Broadband Gateway APNs on page 126

block-visitors

Syntax	block-visitors;
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the access point name (APN) to block visitors who do not belong to the home public land mobile network (HPLMN) from connecting to the APN.</p> <p>When the broadband gateway receives a Create Session Request message from a subscriber's user equipment (UE), the gateway compares the mobile country code (MCC) and the mobile network code (MNC) in the message with the list of configured MCCs and MNCs for the home PLMN. If the user equipment does not belong to the home PLMN, then the gateway rejects the session and the user equipment is blocked from connecting to the APN.</p>
Default	If you do not specify a value, the visitors are allowed by default.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • apns on page 691 • Configuring General APN Parameters on the Broadband Gateway on page 109

count (HTTP Header Enrichment)

Syntax	count;
Hierarchy Level	[edit services hcm tag-rule <i>rule-name</i> term <i>term-name</i> then]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Enable the collection of statistics for the configured term. The collection of statistics for a term is disabled by default.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring HTTP Header Enrichment on page 135• then (HTTP Header Enrichment) on page 750

charging (APN)

Syntax	<pre>charging { default-profile default-profile; home-profile home-profile; profile-selection-order [profile-selection-method]; roamer-profile roamer-profile; visitor-profile visited-profile; }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the charging profiles for the access point name (APN) that will be used to charge the different types of subscribers who access the APN on the broadband gateway. The profile-selection-order configuration indicates the order of preference for the source of the charging profile. If the profile-selection-order configuration indicates static , then the charging profiles specified are used to charge a subscriber.



NOTE: The charging profiles must already be configured on the broadband gateway.

When a subscriber session is created on the APN, a charging profile is applied to the session depending on the type of subscriber (home, visitor, or roamer). The home public land mobile network (HPLMN) configured on the broadband gateway is used to determine the type of subscriber:

- If the subscriber's International Mobile Subscriber Identity (IMSI), mobile country code (MCC), and the mobile network code (MNC) do not match the corresponding values configured for the HPLMN, then the subscriber is deemed a visitor and the **visited-profile** is applied. If the **visited-profile** is not configured, then the **default-profile** is applied.
- If the subscriber's IMSI, MCC, and MNC match the corresponding value configured for the HPLMN, but the subscriber's Routing Area Identity (RAI) does not match the corresponding RAI configured for the HPLMN, then the subscriber is deemed a roamer and the **roamer-profile** is applied. If the **roamer-profile** is not configured, then the **default-profile** is applied.
- If the subscriber is neither a visitor nor a roamer, then the subscriber is deemed a home subscriber and the **home-profile** is applied. If the **home-profile** is not configured, then the **default-profile** is applied.



NOTE: In the absence of a charging profile from all sources, the subscriber session is created without charging enabled.

The remaining statements are explained separately.

Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• apns on page 691• Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 119• charging-profiles on page 780

default-profile

Syntax	<code>default-profile <i>default-profile</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> charging], [edit unified-edge gateways sgw <i>gateway-name</i> charging global-profile]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging global-profile] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Specify the default profile. If the profile-selection-order configuration indicates 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.



NOTE: The charging profile must already be configured on the broadband gateway.

The broadband gateway determines the type of subscriber by using 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) and compares these with the corresponding values configured for the home public land mobile network (HPLMN). Depending on whether a subscriber is a home subscriber, a visitor, or a roamer, the **home-profile**, **visited-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 also not configured, then the subscriber session is created with no charging applied.

Options	<i>default-profile</i> —Name of the default profile.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 119 • Configuring S-GW Global Charging Profiles and Selection Order on page 282 • charging (APN) on page 695 • charging-profiles on page 780 • global-profile (Serving Gateway) on page 806

description (APN)

Syntax	<code>description <i>description</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Enter a description for the access point name (APN).
Options	<i>description</i> —Description of the APN. Range: Up to 80 characters
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• apns on page 691• Configuring General APN Parameters on the Broadband Gateway on page 109

destination-address (HTTP Header Enrichment)

Syntax	<pre>destination-address { (any-unicast any-unicast except); [(<i>prefix</i> <i>prefix</i> except)]; }</pre>
Hierarchy Level	[edit services hcm tag-rule <i>rule-name</i> term <i>term-name</i> from]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Configure the IP address to which to apply the HTTP header extension information. Once this criteria and the other match criteria specified for term are matched, then the actions specified for the term are applied.
Options	any-unicast —Specify that any unicast address is matched. any-unicast except —Specify that all addresses except unicast addresses are matched. <i>prefix</i> —Specify the IP prefix for the addresses that are matched. <i>prefix</i> except —Specify that the addresses except the ones specified in the IP prefix are matched.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring HTTP Header Enrichment on page 135• from (HTTP Header Enrichment) on page 709

destination-address-range (HTTP Header Enrichment)

Syntax	<code>destination-address-range { [high <i>address</i> low <i>address</i>] [except]; }</code>
Hierarchy Level	[edit services hcm tag-rule <i>rule-name</i> term <i>term-name</i> from]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Configure the destination IP address range to which HTTP header enrichment is applied. You can specify multiple address ranges by including the destination-address-range statement multiple times.
Options	<p>high <i>address</i>—Upper limit of the address range.</p> <p>low <i>address</i>—Lower limit of the address range.</p> <p>except—Specify that addresses that are not in the specified address range are matched.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring HTTP Header Enrichment on page 135 • from (HTTP Header Enrichment) on page 709


destination-port-range (HTTP Header Enrichment)

Syntax	<code>destination-port-range { [high <i>port-number</i> low <i>port-number</i>]; }</code>
Hierarchy Level	[edit services hcm tag-rule <i>rule-name</i> term <i>term-name</i> from]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Configure the destination port range to which the HTTP header enrichment is applied. You can specify multiple port ranges by including the destination-port-range statement multiple times.
Options	<p>high <i>port-number</i>—Upper limit of the port range.</p> <p>low <i>port-number</i>—Lower limit of the port range.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring HTTP Header Enrichment on page 135 • from (HTTP Header Enrichment) on page 709

destination-ports (HTTP Header Enrichment)

Syntax	<code>destination-ports [value];</code>
Hierarchy Level	[edit services hcm tag-rule <i>rule-name</i> term <i>term-name</i> from]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Configure the destination ports to which the HTTP header enrichment is applied. You can specify multiple ports by including the destination-ports statement multiple times.
Options	value —Port number. Range: 0 through 65,535
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring HTTP Header Enrichment on page 135• from (HTTP Header Enrichment) on page 709


destination-prefix-list (HTTP Header Enrichment)

Syntax	destination-prefix-list { [(<i>prefix-name</i> <i>prefix-name</i> except)]; }
Hierarchy Level	[edit services hcm tag-rule <i>rule-name</i> term <i>term-name</i> from]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Specify the destination prefix list to which the HTTP header enrichment is applied. You can specify multiple prefix lists by including the destination-prefix-list statement multiple times.
Options	<i>prefix-name</i> —Name of the prefix list.
	<div>  <p>NOTE: The prefix list must already be defined at the [edit policy-options prefix-list] hierarchy level.</p> </div>
	<i>prefix-name</i> except —Specify that the destination addresses not in the specified prefix list are matched.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring HTTP Header Enrichment on page 135 • from (HTTP Header Enrichment) on page 709


dhcp-proxy-client (APN Address Assignment)

Syntax	<pre>dhcp-proxy-client { aaa-override; }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> address-assignment]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the address assignment option so that the IP subnet returned by the Dynamic Host Configuration Protocol (DHCP) server is used by the broadband gateway when it assigns IP addresses for subscribers. If this option is configured, then you must configure a DHCP (IPv4 or IPv6) proxy client profile on the broadband gateway. The broadband gateway uses the information configured in the DHCP proxy client profile to obtain the IP subnet returned by the DHCP server.</p> <p>The remaining statements are explained separately.</p>
Default	If you omit the dhcp-proxy-client statement, the default address assignment option is local . This means that the IP addresses are assigned by the broadband gateway using the mobile pool or mobile pool group configured on the APN. If a mobile pool or a mobile pool group is not specified, then the default mobile pool is used to assign the IP address. The default mobile pool is configured on the routing instance that is associated with the mobile interface of the APN.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• address-assignment (APN) on page 680• Configuring Address Assignment on a Broadband Gateway APN on page 115• Example: Configuring Broadband Gateway APNs on page 126

dhcpv4-proxy-client-profile (APN Address Assignment)

Syntax	<pre>dhcpv4-proxy-client-profile { logical-system <i>logical-system</i>; pool-name <i>pool-name</i>; profile-name <i>profile-name</i>; routing-instance <i>routing-instance</i>; }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> address-assignment]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the Dynamic Host Configuration Protocol (DHCP) IPv4 proxy client profile for the access point name (APN). The broadband gateway uses the DHCP proxy client profile to obtain the subnet or the prefix from the DHCP server for the APN. The subnet or the prefix is managed locally and a single IP address is provided to the user equipment (UE) in the Create Session Response message.
<div style="display: flex; align-items: center;">  <div> <p>NOTE: If you selected <code>dhcp-proxy-client</code> as the mode of address assignment for the broadband gateway, then you must configure a DHCP (IPv4 or IPv6) proxy client profile.</p> </div> </div>	
<p>The remaining statements are explained separately.</p>	
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • address-assignment (APN) on page 680 • Configuring DHCP Under APN on page 209 • Configuring Address Assignment on a Broadband Gateway APN on page 115


dhcipv6-proxy-client-profile (APN Address Assignment)

Syntax	<pre>dhcipv6-proxy-client-profile { logical-system <i>logical-system</i>; pool-name <i>pool-name</i>; profile-name <i>profile-name</i>; routing-instance <i>routing-instance</i>; }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> address-assignment]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the Dynamic Host Configuration Protocol (DHCP) IPv6 proxy client profile for the access point name (APN). The broadband gateway uses the DHCP proxy client profile to obtain the subnet or the prefix from the DHCP server for the APN. The subnet or the prefix is managed locally and a single IP address is provided to the user equipment (UE) in the Create Session Response message.
	<div><p>NOTE: If you selected <code>dhcp-proxy-client</code> as the mode of address assignment for the broadband gateway, then you must configure a DHCP (IPv4 or IPv6) proxy client profile.</p></div>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• address-assignment (APN) on page 680• Configuring DHCP Under APN on page 209• Configuring Address Assignment on a Broadband Gateway APN on page 115


dns-server (APN)

Syntax	<pre> dns-server { primary-v4 <i>primary-v4</i>; primary-v6 <i>primary-v6</i>; secondary-v4 <i>secondary-v4</i>; secondary-v6 <i>secondary-v6</i>; }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the IP addresses of the Domain Name System (DNS) servers for the access point name (APN).</p> <p>During the creation of a session, the user equipment (UE) may request the broadband gateway for the DNS server address. Typically, the gateway obtains this information from the authentication, authorization, and accounting (AAA) server. If the DNS server address is not available from the AAA server, then the gateway sends the DNS server addresses configured for the APN to the user equipment.</p>
Options	<p>primary-v4 <i>primary-v4</i>—IPv4 address of the primary DNS server.</p> <p>primary-v6 <i>primary-v6</i>—IPv6 address of the primary DNS server.</p> <p>secondary-v4 <i>secondary-v4</i>—IPv4 address of the secondary DNS server.</p> <p>secondary-v6 <i>secondary-v6</i>—IPv6 address of the secondary DNS server.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • apns on page 691 • Configuring General APN Parameters on the Broadband Gateway on page 109

encrypt (HTTP Header Enrichment)

Syntax	<pre>encrypt { hash <i>algorithm</i>; prefix <i>hash-prefix</i>; }</pre>
Hierarchy Level	[edit services hcm tag-rule <i>rule-name</i> term <i>term-name</i> then tag <i>tag-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Specify the transform to be applied to the header for the HTTP header enrichment. This allows subscriber attributes to be added in a way that is obscured from the user.
<div> NOTE: If you include this statement, then you also must configure hash and prefix statements.</div>	
Options	<p>hash <i>algorithm</i>—Specify the hashing algorithm. Currently, only md5 is supported.</p> <p>prefix <i>hash-prefix</i>—Specify the prefix key (up to 63 characters). The prefix key is concatenated with the specified tag attribute and hashed. The resulting hash value is then inserted into the HTTP header.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring HTTP Header Enrichment on page 135• tag (HTTP Header Enrichment) on page 742

exclude-pools (APN Address Assignment)

Syntax	<code>exclude-pools [value];</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> address-assignment inet-pool]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the IPv4 mobile pools to exclude from the specified mobile pool group for this access point name (APN). The IP addresses in the excluded mobile pools are not used by the broadband gateway during IP address assignment to subscribers.
	<div>  <p>NOTE: This configuration is valid only when you specify a mobile pool group for the APN.</p> </div>
Options	<p>value—Name of the mobile pool to exclude.</p> <p>To specify multiple mobile pools to exclude, include the exclude-pools statement multiple times.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Address Assignment on a Broadband Gateway APN on page 115 • inet-pool (APN Address Assignment) on page 716

exclude-v6pools (APN Address Assignment)

Syntax	<code>exclude-v6pools [value];</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> address-assignment inet6-pool]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the IPv6 mobile pools to exclude from the specified mobile pool group for this access point name (APN). The IP addresses in excluded mobile pools are not used by the broadband gateway during IP address assignment to subscribers.



NOTE: This configuration is valid only when you specify a mobile pool group for the APN.

Options	value —Name of the mobile pool to exclude. To specify multiple mobile pools to exclude, include the exclude-v6pools statement multiple times.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Address Assignment on a Broadband Gateway APN on page 115• inet6-pool (APN Address Assignment) on page 717

from (HTTP Header Enrichment)

```
Syntax  from {
        destination-address {
            (any-unicast | any-unicast except);
            [prefix];
        }
        destination-address-range {
            [high address low address] [except];
        }
        destination-port-range {
            [high port-number low port-number];
        }
        destination-ports [value];
        destination-prefix-list {
            (prefix-name | prefix-name except);
        }
    }
```

Hierarchy Level [edit services hcm tag-rule *rule-name* term *term-name*]

Release Information Statement introduced in Junos OS Mobility Release 11.4W.

Description Specify the match criteria for the term. If all the conditions specified in the match criteria are met, then the actions specified in the **then** statement are applied.



NOTE: You must configure this statement and include at least one match criterion.


The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring HTTP Header Enrichment on page 135](#)
- [term \(HTTP Header Enrichment\) on page 749](#)

group (APN Address Assignment)

Syntax	<code>group group;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> address-assignment inet-pool], [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> address-assignment inet6-pool]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify a previously configured mobile pool group (IPv4 or IPv6) for the access point name (APN). The broadband gateway uses the mobile pool group to assign IP addresses locally to subscribers.
	<div> NOTE: You can specify either a mobile pool group or a mobile pool, but not both.</div>
Default	If neither a mobile pool nor mobile group is specified, then the default mobile pool is used to assign the IP address. The default mobile pool is configured in the routing instance that is associated with the mobile interface of the APN.
Options	<i>group</i> —Name of the mobile pool group.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Address Assignment on a Broadband Gateway APN on page 115• inet-pool (APN Address Assignment) on page 716• inet6-pool (APN Address Assignment) on page 717• mobile-pool-groups on page 622

hcm (HTTP Header Enrichment)

```

Syntax  hcm {
        tag-attribute [attr-name];
        tag-rule rule-name {
            term term-name {
                from {
                    destination-address {
                        (any-unicast | any-unicast except);
                        [prefix];
                    }
                    destination-address-range {
                        [high address low address] [except];
                    }
                    destination-port-range {
                        [high port-number low port-number];
                    }
                    destination-ports [value];
                    destination-prefix-list {
                        (prefix-name | prefix-name except);
                    }
                }
            }
            then {
                count;
                tag tag-name {
                    encrypt {
                        hash algorithm;
                        prefix hash-prefix;
                    }
                    tag-attribute tag-attr-name;
                    tag-header header;
                    tag-separator separator;
                }
            }
        }
    }
    tag-rule-set rule-set-name {
        [rule rule-name];
    }
}

```

Hierarchy Level [edit services]

Release Information Statement introduced in Junos OS Mobility Release 11.4W.

Description Configure the parameters required to support Hypertext Transfer Protocol (HTTP) header enrichment on the broadband gateway.

The broadband gateway can support content added to the 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).

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [\[edit services hcm\] Hierarchy Level on page 558](#)
- [Configuring HTTP Header Enrichment on page 135](#)

home-profile

Syntax `home-profile home-profile;`

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name* apn-services apns *name* charging],
[edit unified-edge gateways sgw *gateway-name* charging global-profile]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.
Support at the [edit unified-edge gateways sgw *gateway-name* charging global-profile]
hierarchy level introduced in Junos OS Mobility Release 11.4W.

Description Specify the profile that should be used to charge home subscribers. If the **profile-selection-order** configuration indicates **static**, then this profile is used for home subscribers.



.....

NOTE: The charging profile must already be configured on the broadband gateway.

.....

The broadband gateway determines whether the subscriber is a home subscriber by using 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). If the subscriber's International Mobile Subscriber Identity (IMSI), MCC, and MNC belong to the same PLMN to which both the GGSN or P-GW and the S-GW belong, then the subscriber is deemed a home subscriber and the **home-profile** is applied. If the **home-profile** is not configured, then the **default-profile**, if configured, is applied. If the **default-profile** is also not configured, then the subscriber session is created with no charging applied.

Options *home-profile*—Name of the home profile.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.


Related Documentation

- [Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 119](#)
- [Configuring S-GW Global Charging Profiles and Selection Order on page 282](#)
- [charging \(APN\) on page 695](#)
- [charging-profiles on page 780](#)
- [global-profile \(Serving Gateway\) on page 806](#)


idle-timeout (APN)

Syntax	<code>idle-timeout <i>idle-timeout</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the idle timeout for the access point name (APN). The idle timeout is the duration that the packet data protocol (PDP) context or bearer waits to receive a data packet before timing out. After the idle timeout expires, the broadband gateway takes down the PDP context or bearer. Setting the idle timeout ensures that if no data is being sent for the duration specified, then the PDP context and bearers can be taken down, and the gateway's resources can be freed.
Options	<p><i>idle-timeout</i>—Idle timeout for the APN.</p> <p>Range: 0 through 300 minutes</p> <p>Default: 0 minutes indicates that idle timeout will not be detected. PDP contexts or bearers will remain active indefinitely even if there is no data being transmitted.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • apns on page 691 • Configuring General APN Parameters on the Broadband Gateway on page 109 • idle-timeout-direction (APN) on page 714


idle-timeout-direction (APN)

Syntax	idle-timeout-direction (both uplink);
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the direction of the traffic (uplink or both uplink and downlink) to be considered for idle timeout for the access point name (APN).
	<div><p>NOTE: The <code>idle-timeout-direction</code> is applicable only if you have configured an <code>idle-timeout</code> value.</p></div>
Default	If you do not specify an option, both is considered the default timeout direction; that is, the idle period is detected in both the uplink and downlink direction.
Options	both —Detect the idle periods for data traffic flowing in both uplink and downlink directions. uplink —Detect the idle periods for data traffic flowing only in the uplink direction.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• apns on page 691• Configuring General APN Parameters on the Broadband Gateway on page 109• idle-timeout (APN) on page 713


imsi (Network Behind Mobile)

Syntax	<pre>imsi <i>imsi</i> { <i>prefix-v4</i> [<i>ipv4-prefix</i>]; <i>prefix-v6</i> [<i>ipv6-prefix</i>]; }</pre>
Hierarchy Level	[edit unified-edge gateways <i>ggsn-pgw gateway-name</i> apn-services apns <i>name</i> network-behind-mobile]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Specify the International Mobile Subscriber Identity (IMSI) of the user equipment (UE). The broadband gateway uses the IMSI to map the configured prefixes to a GPRS tunneling protocol (GTP) tunnel and forwards the traffic to the devices behind the user equipment.
	<div>  <p>NOTE: If you configure the <code>imsi</code> statement, you must specify either the IPv4 prefix, the IPv6 prefix, or both prefixes.</p> </div> <p>The remaining statements are explained separately.</p>
Options	<p><i>imsi</i>—IMSI of the user equipment.</p> <p>To configure multiple IMSIs, include the imsi statement multiple times.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring the Networks Behind the Mobile Equipment Feature on page 131 • network-behind-mobile on page 725

inet-pool (APN Address Assignment)

Syntax	<pre>inet-pool { exclude-pools [value]; group group; pool pool; }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> address-assignment]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Specify the IPv4 mobile pool or mobile pool group that will be used by the broadband gateway to assign IP addresses locally to subscribers. If you specify a mobile pool group, you can also configure a set of mobile pools to be excluded from the access point name (APN).</p> <p>You configure the inet-pool if you selected local as the mode of address assignment for the broadband gateway.</p> <div> NOTE: You can specify either a mobile pool group or a mobile pool, but not both.</div> <p>The remaining statements are explained separately.</p>
Default	If neither a mobile pool nor a mobile group is specified, then the default mobile pool is used to assign the IP address. The default mobile pool is configured in the routing instance that is associated with the mobile interface of the APN.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• address-assignment (APN) on page 680• Configuring Address Assignment on a Broadband Gateway APN on page 115


inet6-pool (APN Address Assignment)

Syntax	<pre>inet6-pool { exclude-v6pools [value]; group group; pool pool; }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> address-assignment]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Specify the IPv6 mobile pool or mobile pool group that will be used by the broadband gateway to assign IP addresses locally to subscribers. If you specify a mobile pool group, you can also configure a set of mobile pools to be excluded from the access point name (APN).</p> <p>You configure the inet6-pool if you selected local as the mode of address assignment for the broadband gateway.</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;">  <p>NOTE: You can specify either a mobile pool group or a mobile pool, but not both.</p> </div> <p>The remaining statements are explained separately.</p>
Default	If neither a mobile pool nor mobile group is specified, then the default mobile pool is used to assign the IP address. The default mobile pool is configured in the routing instance that is associated with the mobile interface of the APN.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • address-assignment (APN) on page 680 • Configuring Address Assignment on a Broadband Gateway APN on page 115


inter-mobile-traffic (APN)

Syntax	<pre>inter-mobile-traffic { (deny redirect <i>redirect</i>); }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the inter-mobile traffic options for the access point name (APN).</p> <p>Inter-mobile traffic refers to the traffic between two user equipment (UE) that are anchored on the broadband gateway. You can either deny inter-mobile traffic, which means that the gateway will drop the inter-mobile traffic, or redirect the inter-mobile traffic through the configured IP address.</p>
Options	<p>deny—Do not allow inter-mobile traffic.</p> <p>redirect <i>redirect</i>—IPv4 address to which the inter-mobile traffic should be redirected.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• apns on page 691• Configuring General APN Parameters on the Broadband Gateway on page 109

local (APN Address Assignment)

Syntax	local { aaa-override; }
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> address-assignment]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the address assignment option so that the broadband gateway assigns IP addresses locally to subscribers. The gateway assigns addresses using the mobile pool or mobile pool group previously configured on the access point name (APN).
	<div>  <p>NOTE: An APN can have a mobile pool or a mobile pool group configured, but not both.</p> </div> <p>The remaining statement is explained separately.</p>
Default	If you do not specify any option, the default address assignment option is local . If a mobile pool or a mobile pool group is not specified, then the default mobile pool is used to assign the IP address. The default mobile pool is configured in the routing instance that is associated with the mobile interface of the APN.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • address-assignment (APN) on page 680 • Configuring AAA-Assigned Addresses to Override Locally or DHCP-Assigned Addresses on page 191

local-policy-profile (APN)

Syntax	<code>local-policy-profile <i>local-policy-profile</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify a local policy for the access point name (APN) on the broadband gateway. The local policy is a combination of the quality-of-service (QoS) policy (cos-policy-profile), the classifier policy (classifier-profile), and the resource threshold policy (resource-threshold-policy). The local policy specified for the APN takes precedence over the one specified for the gateway.
	<div> NOTE: The local-policy-profile must already be configured at the [edit unified-edge] hierarchy level.</div>
Default	If you do not specify a local policy for the APN, then the local policy specified for the gateway is applied.
Options	<i>local-policy-profile</i> —Name of local policy profile.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• apns on page 691• Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 119• local-policy-profile (Broadband Gateway) on page 878

logical-system (APN Address Assignment)

Syntax	<code>logical-system <i>logical-system</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> address-assignment dhcpv4-proxy-client-profile], [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> address-assignment dhcpv6-proxy-client-profile]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the logical system where the Dynamic Host Configuration Protocol (DHCP) proxy client profile (IPv4 or IPv6) is defined.
Default	If you do not configure this statement, then the default logical system configured is used.
Options	<i>logical-system</i> —Name of the logical system where the DHCP proxy client profile is defined.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring DHCP Under APN on page 209 • Configuring Address Assignment on a Broadband Gateway APN on page 115 • dhcpv4-proxy-client-profile (APN Address Assignment) on page 703 • dhcpv6-proxy-client-profile (APN Address Assignment) on page 704

maximum-bearers (APN)

Syntax	<code>maximum-bearers <i>maximum-bearers</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the maximum number of bearers or packet data protocol (PDP) contexts allowed for the access point name (APN). The maximum number of bearers specified for the APN takes precedence over the corresponding value specified for the gateway.
Default	If you do not configure the maximum-bearers for the APN, then the maximum bearers allowed for the APN is limited by the maximum-bearers configured for the gateway.
Options	<i>maximum-bearers</i> —Maximum number of bearers for the APN. Range: 100,000 through 12,000,000 bearers
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• apns on page 691• Configuring General APN Parameters on the Broadband Gateway on page 109• Configuring the Maximum Number of Bearers on page 324• maximum-bearers (Broadband Gateway) on page 880

mobile-interface (APN)

Syntax	<code>mobile-interface <i>mobile-interface</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the mobile interface for the access point name (APN).

A class of subscribers is represented by a logical interface (**ifl**) template. This logical interface template is configured in the mobile interface (**interfaces mif**) hierarchy level. The APN is associated with the mobile logical interface (**mif**) template through this configuration. Therefore, all subscribers in this APN will execute the common features, such as a firewall, in the **mobile-ifl** context.



NOTE: The configuration of a mobile interface is mandatory.

Options `mobile-interface`—Mobile interface name.



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

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

- Related Documentation**
- [apns on page 691](#)
 - [Configuring General APN Parameters on the Broadband Gateway on page 109](#)
 - [Configuring Mobile Interfaces for APNs on page 120](#)
 - [interfaces \(Mobile Interface\) on page 990](#)

nbns-server (APN)

Syntax	<pre>nbns-server { primary-v4 <i>primary-v4</i>; secondary-v4 <i>secondary-v4</i>; }</pre>
Hierarchy Level	[edit unified-edge gateways <i>ggsn-pgw gateway-name</i> apn-services apns <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the NetBIOS name server (NBNS) servers for the access point name (APN).</p> <p>During the creation of a session, the user equipment (UE) may request the NBNS server address from the broadband gateway. Typically, the gateway obtains this information from the authentication, authorization, and accounting (AAA) server. If the NBNS server address is not available from the AAA server, the gateway sends the NBNS server addresses configured for the APN to the user equipment.</p>
Options	<p>primary-v4 <i>primary-v4</i>—IPv4 address of the primary NBNS server.</p> <p>secondary-v4 <i>secondary-v4</i>—IPv4 address of the secondary NBNS server.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• apns on page 691• Configuring General APN Parameters on the Broadband Gateway on page 109

network-behind-mobile

Syntax	<pre>network-behind-mobile { imsi imsi { prefix-v4 [ipv4-prefix]; prefix-v6 [ipv6-prefix]; } }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	<p>Specify the configuration for network behind mobile for the access point name (APN). The broadband gateway acts as the IP anchor for devices that are behind the user equipment and forwards traffic to and from these devices. The broadband gateway determines the network prefixes or IP addresses for the devices behind the user equipment either from the prefixes configured for the APN or from the Access Accept messages from the authentication, authorization, and accounting (AAA) server.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • allow-network-behind-mobile on page 681 • Configuring the Networks Behind the Mobile Equipment Feature on page 131


no-address-verify (APN Address Assignment)

Syntax	no-address-verify;
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> address-assignment allow-static-ip-address]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify that the static IP address provided by the user equipment (UE) is not verified by the broadband gateway.
Default	If you omit the no-address-verify statement, then the static IP address provided by the user equipment is verified with the authentication, authorization, and accounting (AAA) server during the authentication phase.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • allow-static-ip-address (APN Address Assignment) on page 682 • Configuring Address Assignment on a Broadband Gateway APN on page 115


p-cscf (APN)

Syntax	<pre>p-cscf { [address]; }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the IPv4 or IPv6 address of the proxy-call session control function (P-CSCF) server, which is used for IP Multimedia Subsystem (IMS) calls.</p> <p>During the creation of a session, the user equipment (UE) can request the P-CSCF server's address from the broadband gateway. Typically, the gateway obtains this information from the authentication, authorization, and accounting (AAA) server. If the P-CSCF server's address is not available from the AAA server, the gateway sends the P-CSCF server's address configured for the APN to the user equipment.</p>
Options	<p>address—IP address (IPv4 and/or IPv6) of the P-CSCF server.</p> <p>To specify multiple addresses, include the p-cscf statement multiple times.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• apns on page 691• Configuring General APN Parameters on the Broadband Gateway on page 109


prefix-v4 (Network Behind Mobile)

Syntax	<code>prefix-v4 [ipv4-prefix];</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> network-behind-mobile imsi <i>imsi</i>]
Description	Configure the IPv4 prefixes for the devices behind the user equipment.
<div>  <p>NOTE:</p> <ul style="list-style-type: none"> • If you configure the <code>imsi</code> statement, you must specify either the IPv4 prefix, the IPv6 prefix, or both prefixes. • You can configure maximum of 32 prefixes (only IPv4, only IPv6, or both IPv4 and IPv6). • By default, the IPv4 prefixes configured using this statement take precedence over the information returned by the authentication, authorization, and accounting (AAA) server. However, if the access point name's address assignment is configured to use the local pool and if the <code>aaa-override</code> statement is also specified, then the prefixes configured using this statement are overwritten by the information obtained from the AAA server. </div>	
Options	<p><code>ipv4-prefix</code>—IPv4 prefix of the device.</p> <p>To configure multiple IPv4 prefixes, include the <code>prefix-v4</code> statement multiple times.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring the Networks Behind the Mobile Equipment Feature on page 131 • imsi (Network Behind Mobile) on page 715

prefix-v6 (Network Behind Mobile)

Syntax	<code>prefix-v6 [ipv6-prefix];</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw gateway-name apn-services apns name network-behind-mobile imsi <i>imsi</i>]
Description	Configure the IPv6 prefixes for the devices behind the user equipment. The MobileNext Broadband Gateway uses these prefixes to forward traffic to and from the devices behind the user equipment.
	<div><div></div><div><p>NOTE:</p><ul style="list-style-type: none">• If you configure the <code>imsi</code> statement, you must specify either the IPv4 prefix, the IPv6 prefix, or both prefixes.• You can configure maximum of 32 prefixes (only IPv4, only IPv6, or both IPv4 and IPv6).• By default, the IPv6 prefixes configured using this statement take precedence over the information returned by the authentication, authorization, and accounting (AAA) server. However, if the access point name's address assignment is configured to use the local pool and if the <code>aaa-override</code> statement is also specified, then the prefixes configured using this statement are overwritten by the information obtained from the AAA server.</div></div>
Options	<p><code>ipv6-prefix</code>—IPv6 prefix of the device.</p> <p>To configure multiple IPv6 prefixes, include the prefix-v6 statement multiple times.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring the Networks Behind the Mobile Equipment Feature on page 131• imsi (Network Behind Mobile) on page 715


pool (APN Address Assignment)

Syntax	<code>pool <i>pool</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> address-assignment inet-pool], [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> address-assignment inet6-pool]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify a mobile pool (IPv4 or IPv6) for the access point name (APN). The broadband gateway uses the mobile pool to assign IP addresses locally to subscribers. The mobile pool that you specify must already be configured on the broadband gateway.
	<div>  <p>NOTE: You can specify either a mobile pool or a mobile pool group, but not both.</p> </div>
Default	If neither a mobile pool nor mobile group is specified, then the default mobile pool is used to assign the IP address. The default mobile pool is configured in the routing instance that is associated with the mobile interface of the APN.
Options	<i>pool</i> —Name of the pool.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Address Assignment on a Broadband Gateway APN on page 115 • inet-pool (APN Address Assignment) on page 716 • inet6-pool (APN Address Assignment) on page 717 • mobile-pools on page 623


pool-name (APN Address Assignment)

Syntax	<code>pool-name <i>pool-name</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> address-assignment dhcpv4-proxy-client-profile], [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> address-assignment dhcpv6-proxy-client-profile]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the name of the pool to be sent to the Dynamic Host Configuration Protocol (DHCP) server. The DHCP server returns a subnet for the access point name (APN) from the specified pool. This parameter is optional.
Options	<i>pool-name</i> —Name of the pool to be sent to the DHCP server.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring DHCP Under APN on page 209• Configuring Address Assignment on a Broadband Gateway APN on page 115• dhcpv4-proxy-client-profile (APN Address Assignment) on page 703• dhcpv6-proxy-client-profile (APN Address Assignment) on page 704

profile-name (APN Address Assignment)

Syntax	<code>profile-name <i>profile-name</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> address-assignment dhcpv4-proxy-client-profile], [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> address-assignment dhcpv6-proxy-client-profile]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the Dynamic Host Configuration Protocol (DHCP) proxy client profile (IPv4 or the IPv6) for the access point name (APN). The profile name under a specific or the default logical system, and a specific or the default routing instance are used when the gateway requests the DHCP server for subnets for the APN.
<div>  <p>NOTE: The proxy client profile must be previously configured on the broadband gateway. This configuration is done when you configure address pools for mobile subscribers.</p> </div>	
Options	<i>profile-name</i> —Name of the DHCP proxy client profile.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring DHCP Under APN on page 209 • Configuring Address Assignment on a Broadband Gateway APN on page 115 • dhcpv4-proxy-client-profile (APN Address Assignment) on page 703 • dhcpv6-proxy-client-profile (APN Address Assignment) on page 704 • mobile-pools on page 623

profile-selection-order (APN)

Syntax	<code>profile-selection-order [<i>profile-selection-method</i>];</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> charging]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Specify the order of the methods used to select a charging profile applicable for a subscriber's session. You can specify a maximum of three profile selection methods—radius, static, or serving. If the first choice is not available, then the next choice is considered, and so on.</p> <p>For example, consider a scenario where the profile selection order is radius, serving, and static. Since radius is the first choice, the charging profile provided by the authentication, authorization, and accounting (AAA) server will be used. If the AAA server does not provide a charging profile ID in the Authentication Accept message, then the next choice (serving) is considered. If the Serving GPRS Support Node (SGSN) does not provide a charging profile ID in the charging characteristics information element (IE) within the GPRS tunneling protocol (GTP) Create Session message, then the next choice (static) is considered. With the static option, the charging profiles that you specified on the access point name (APN) are used to charge the subscriber based on subscriber's status (home, visitor, or roamer).</p>
	<div>  <p>NOTE: If the charging profile cannot be selected by any of the methods specified, then charging is disabled for that subscriber.</p> </div>
Options	<p><i>profile-selection-method</i>—One or more profile selection methods, listed in the order in which they should be tried. The method can be one or more of the following:</p> <ul style="list-style-type: none"> • radius—Use the charging profile sent by the AAA server. • serving—Use the charging profile sent by the SGSN or the Serving Gateway (S-GW). • static—Use the charging profile configured locally for the APN on the broadband gateway.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 119 • charging (APN) on page 695

restriction-value (APN)

Syntax	<code>restriction-value <i>restriction-value</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the restriction value for the access point name (APN) based on the applications allowed on this APN and on other APNs configured on the broadband gateway. When you configure a restriction value for an APN, the restriction value determines the traffic that can be sent by a subscriber on that APN to other APNs. For example, subscribers cannot send Wireless Application Protocol (WAP) or Multimedia Messaging Service (MMS) messages to subscribers on an APN that does not support MMS or WAP.

[Table 53 on page 733](#) displays the valid restriction values that you can configure.

Table 53: Valid Restriction Values for APNs

Maximum APN Restriction Value	Type of APN	Application Example	Allowed Restriction Values on Other APNs
0	Not applicable (no restriction)	Not applicable (no restriction)	All
1	Public Type 1	WAP or MMS	1,2, or 3
2	Public Type 1	Internet or other Packet Data Network (PDN)	1 or 2
3	Private Type 1	Corporate network MMS	1
4	Private Type 2	Corporate network without MMS	None

Options	<p><i>restriction-value</i>—Restriction value for the APN.</p> <p>Range: 0 through 4</p> <p>Default: 0 indicates that there are no restrictions on the traffic sent from one APN to another.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • apns on page 691 • Configuring the Restriction Value on a Broadband Gateway APN on page 113

roamer-profile

Syntax	<code>roamer-profile <i>roamer-profile</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> charging], [edit unified-edge gateways sgw <i>gateway-name</i> charging global-profile]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging global-profile] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Configure the profile that should be used to charge roaming subscribers. If the profile-selection-order configuration indicates static , then this profile is used for roaming subscribers.



NOTE: The charging profile must already be configured on the broadband gateway.

The broadband gateway determines whether the subscriber is a roamer by using 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). If the subscriber's International Mobile Subscriber Identity (IMSI), MCC, and MNC belong to the same PLMN as the GGSN or P-GW, but the S-GW belongs to a different PLMN, then the subscriber is deemed a roamer and the **roamer-profile** is applied. If the **roamer-profile** is not configured, then the **default-profile**, if configured, is applied. If the **default-profile** is also not configured, then the subscriber session is created with no charging applied.

Options	<i>roamer-profile</i> —Name of the roamer profile.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 119• Configuring S-GW Global Charging Profiles and Selection Order on page 282• charging (APN) on page 695• charging-profiles on page 780• global-profile (Serving Gateway) on page 806

routing-instance (APN Address Assignment)

Syntax	<code>routing-instance <i>routing-instance</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> address-assignment dhcpv4-proxy-client-profile], [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> address-assignment dhcpv6-proxy-client-profile]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the routing instance where the Dynamic Host Configuration Protocol (DHCP) proxy client profile (IPv4 or IPv6) is defined.
Default	If you do not configure this statement, then the default routing instance configured is used.
Options	<i>routing-instance</i> —Routing instance where the DHCP proxy client profile is defined.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring DHCP Under APN on page 209 • Configuring Address Assignment on a Broadband Gateway APN on page 115 • dhcpv4-proxy-client-profile (APN Address Assignment) on page 703 • dhcpv6-proxy-client-profile (APN Address Assignment) on page 704

rule (Tag Rule Set)

Syntax	[rule <i>rule-name</i>];
Hierarchy Level	[edit services hcm tag-rule-set]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Specify the tag rule that should be a part of the tag rule set.



.....

NOTE: The tag rule must already be defined at the [edit services hcm] hierarchy level.

.....

Options	<i>rule-name</i> —Name of the tag rule. To specify multiple tag rules, include the rule statement multiple times.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring HTTP Header Enrichment on page 135• tag-rule-set (HTTP Header Enrichment) on page 747

selection-mode (APN)

Syntax `selection-mode {
 (from-ms | from-sgsn | no-subscribed);
 }`

Hierarchy Level `[edit unified-edge gateways ggsn-pgw gateway-name apn-services apns name]`

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the access point name (APN) to support the use of the Selection Mode information element (IE) in the Create Session Request or the Create Packet Data Protocol (PDP) Context message. The broadband gateway accepts or rejects the activation of the bearer or the PDP context depending on the **selection-mode** configured. [Table 54 on page 737](#) displays the selection mode IE values and their descriptions.

The following selection mode options can be configured for the APN:

- **from-ms**—If you configure this option, then the broadband gateway allows the Create Session Request or Create PDP Context message with the selection mode IE value of 1.
- **from-sgsn**—If you configure this option, then the broadband gateway allows the Create Session Request or Create PDP Context message with the selection mode IE value of 2 or 3.
- **no-subscribed**—If you configure this option, then the broadband gateway rejects the Create Session Request or Create PDP Context message with the selection mode IE value of 0.

Table 54: Selection Mode Values

Description	Value
MS-provided or network-provided APN, subscription verified	0
MS-provided APN, subscription not verified	1
Network-provided APN, subscription not verified	2
For future use.	3

NOTE: This selection mode should not be sent. However, if it is received, then its value is interpreted as 2.

Default If you do not configure this statement, then the broadband gateway allows the Create Session Request or Create PDP Context message with the selection mode IE value of 0.

Options **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.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [apns on page 691](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 109](#)

service-mode (APN)

Syntax `service-mode service-mode-options;`

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name* apn-services apns *name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify that the access point name (APN) should be in **maintenance** mode. You do this if you want to carry out maintenance tasks like deleting an APN or changing the APN type and so on. See the *Maintenance Mode* chapter in the *MobileNext Broadband Gateway Configuration Guide* for a list of the maintenance tasks that can be carried out when the APN is in maintenance mode.

When in the **Maintenance Mode Active Phase**, all the valid attributes on the object can be modified. In other cases, only the non-maintenance mode attributes can be modified.


Options *service-mode-options*—Specify the service mode. Currently, **maintenance** mode is the only option supported.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [apns on page 691](#)
- [Configuring the Mobile Interface of an Access Point Name on page 399](#)
- [Deleting an Access Point Name on page 401](#)
- [Example: Changing Access Point Name Values on page 411](#)
- [Modifying an Access Point Name on page 398](#)

service-selection-profile (APN)

Syntax	<code>service-selection-profile <i>service-selection-profile</i>;</code>
Hierarchy Level	<code>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i>]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the service selection profile to be used for the access point name (APN). Service selection profiles specify how services are applied to a subscriber. Service selection profiles are used to redirect subscribers to a peer, or to map a virtual APN to a real APN.
	 <p>NOTE: The service selection profile must be already configured on the broadband gateway.</p>
Options	<code><i>service-selection-profile</i></code> —Service selection profile for the APN.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • apns on page 691 • Configuring APN Service Selection on a Broadband Gateway on page 123 • service-selection-profiles on page 765

service-set-options

Syntax	<pre>service-set-options { <i>subscriber-awareness</i>; }</pre>
Hierarchy Level	<code>[edit services service-set <i>service-set-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 10.1.
Description	<p>Specify the service set options to apply to a service set. These options are used to indicate to the mobility control plane infrastructure that the services PIC should be programmed with the subscriber data on receipt of a Create Subscriber Request message.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • service-set (Aggregated Multiservices) on page 978

session-timeout (APN)

Syntax	<code>session-timeout session-timeout;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the session timeout for the access point name (APN). The session timeout is the period that a default bearer or a primary packet data protocol (PDP) context is active (with or without receiving data packets) before timing out. When the configured session timeout expires, the broadband gateway deactivates the default bearer or the primary PDP context.
Options	<p><i>session-timeout</i>—Session timeout for the APN.</p> <p>Range: 0 through 720 hours</p> <p>Default: 0 hours indicates that session timeout will not be enabled for the APN.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• apns on page 691• Configuring General APN Parameters on the Broadband Gateway on page 109

subscriber-awareness (Service Set Options)

Syntax	subscriber-awareness;
Hierarchy Level	[edit services service-set <i>service-set-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	<p>Enable subscriber awareness on the service set.</p> <p>To provide subscriber-aware services, you must configure the subscriber-aware statement on the service set. This is a prerequisite for obtaining mobility subscriber-aware services on the service set. For subscriber-aware HTTP header enrichment (HTTP HE) services for mobility, the service set containing the HTTP HE rules must be configured as subscriber-aware.</p> <p>Configuring a service set as subscriber-aware allows services to obtain subscriber-specific information. In the case of HTTP HE, the subscriber-specific information is the Mobile Station ISDN (MSISDN) number or the International Mobile Subscriber Identity (IMSI) of the mobile subscriber. Configuring a service set as subscriber-aware enables the HTTP HE service to correlate the HTTP connections with the correct subscriber and insert the subscriber's corresponding IMSI or MSISDN into the HTTP header, as configured in the HTTP HE rules.</p>
Default	If you do not include the subscriber-awareness statement, then mobility subscriber-aware services cannot be provided.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring HTTP Header Enrichment on page 135 • service-set-options on page 739


tag (HTTP Header Enrichment)

Syntax	<pre>tag <i>tag-name</i> { encrypt { hash <i>algorithm</i>; prefix <i>hash-prefix</i>; } tag-attribute <i>tag-attr-name</i>; tag-header <i>header</i>; tag-separator <i>separator</i>; }</pre>
Hierarchy Level	[edit services hcm tag-rule <i>rule-name</i> term <i>term-name</i> then]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the tags to be applied to the HTTP headers matching the criteria specified in the from statement. If you configure a tag, you must include the tag-header statement.</p> <p>The remaining statements are explained separately.</p>
Options	<i>tag-name</i> —Name of the tag.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring HTTP Header Enrichment on page 135• then (HTTP Header Enrichment) on page 750

tag-attribute (HTTP Header Enrichment)

Syntax	<code>tag-attribute [attr-name];</code>
Hierarchy Level	[edit services hcm]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	<p>Specify the list of tag attributes to be used for the tag rules for HTTP header enrichment.</p> <p>These attributes are stored in the subscriber database for mobile subscribers. Once these attributes are configured, they can be used in the tag rules. HTTP tag rules can be configured to choose one or more of these attributes to insert in the HTTP header.</p>
Options	<p><i>attr-name</i>—Tag attribute. To specify multiple attributes at one time, include the attributes in square brackets ([]). The supported mobile attributes are imsi and msisdn.</p> <p>Values: Up to 63 characters</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring HTTP Header Enrichment on page 135 • hcm (HTTP Header Enrichment) on page 711

tag-attribute (HTTP Header Enrichment Tag)

Syntax	<code>tag-attribute [tag-attr-name];</code>
Hierarchy Level	[edit services hcm tag-rule <i>rule-name</i> term <i>term-name</i> then tag <i>tag-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Specify the tag attribute (for the tag header and separator) to insert into the HTTP header.
	<div style="display: flex; align-items: flex-start;"> <div style="flex: 1; text-align: center;">  </div> <div style="flex: 3; padding-left: 10px;"> <p>NOTE: The tag attribute specified here must already be defined at the [edit services hcm] hierarchy level.</p> </div> </div>
Options	<i>tag-attr-name</i> —Tag attribute.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring HTTP Header Enrichment on page 135 • tag (HTTP Header Enrichment) on page 742

tag-header (HTTP Header Enrichment)

Syntax	<code>tag-header header;</code>
Hierarchy Level	[edit services hcm tag-rule <i>rule-name</i> term <i>term-name</i> then tag <i>tag-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Specify the tag header for the tag to be inserted into the HTTP header. This is a required configuration.
Options	<i>header</i> —Tag header. Values: Up to 63 characters
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring HTTP Header Enrichment on page 135• tag (HTTP Header Enrichment) on page 742

tag-rule (HTTP Header Enrichment)

```
Syntax  tag-rule rule-name {
        term term-name {
            from {
                destination-address {
                    (any-unicast | any-unicast except);
                    [prefix];
                }
                destination-address-range {
                    [high address low address] [except];
                }
                destination-port-range {
                    [high port-number low port-number];
                }
                destination-ports [value];
                destination-prefix-list {
                    (prefix-name | prefix-name except);
                }
            }
            then{
                count;
                tag tag-name {
                    encrypt {
                        hash algorithm;
                        prefix hash-prefix;
                    }
                    tag-attribute tag-attr-name;
                    tag-header header;
                    tag-separator separator;
                }
            }
        }
    }
```

Hierarchy Level [edit services hcm]

Release Information Statement introduced in Junos OS Mobility Release 11.4W.

Description Configure the tag rules that the broadband gateway uses to determine which HTTP headers are enriched with the appropriate tags.


Options *rule-name*—Name of the tag rule.
Values: 1 through 63 characters

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring HTTP Header Enrichment on page 135](#)
- [hcm \(HTTP Header Enrichment\) on page 711](#)


tag-rules (HTTP Header Enrichment)

Syntax	[tag-rules <i>rule-name</i>];
Hierarchy Level	[edit services service-set <i>service-set-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	<p>Specify one or more tag rules to apply to a service set.</p> <p>The tag rules are matched in the order that they are configured. If a rule is matched, then the actions specified in the tag rule are applied and the subsequent tag rules are skipped.</p>
Options	<p><i>rule-name</i>—Name of the tag rule.</p> <p>You can specify multiple tag rules by including the tag-rules statement multiple times.</p>
	<div><p>NOTE: The tag rules must already be defined at the [edit services hcm] hierarchy level.</p></div>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring HTTP Header Enrichment on page 135• service-set (Aggregated Multiservices) on page 978

tag-rule-set (HTTP Header Enrichment)

Syntax	<code>tag-rule-set <i>rule-set-name</i> { [<i>rule rule-name</i>]; }</code>
Hierarchy Level	[edit services hcm]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Configure the tag rule set for HTTP header enrichment. You do this to group multiple configured tag rules into one tag rule set.
Options	<p><i>rule-set-name</i>—Name of the tag rule set.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring HTTP Header Enrichment on page 135• hcm (HTTP Header Enrichment) on page 711

tag-rule-sets (HTTP Header Enrichment)

Syntax	[tag-rule-sets <i>rule-set-name</i>];
Hierarchy Level	[edit services service-set <i>service-set-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Specify one or more tag rule sets to apply to a service set. If you have multiple tag rules to match, you can combine them together into a single tag rule set that can then be used across multiple service sets.
Options	<i>rule-set-name</i> —Name of the tag rule set. You can specify multiple tag rule sets by including the tag-rule-sets statement multiple times.
	<div> NOTE: The tag rule set must already be defined at the [edit services hcm] hierarchy level.</div>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring HTTP Header Enrichment on page 135• service-set (Aggregated Multiservices) on page 978

tag-separator (HTTP Header Enrichment)

Syntax	tag-separator <i>separator</i> ;
Hierarchy Level	[edit services hcm tag-rule <i>rule-name</i> term <i>term-name</i> then tag <i>tag-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Specify the tag separator for the tag to be inserted into the HTTP header.
Options	<i>separator</i> —Tag separator. Syntax: 1 character Default: / (forward slash)
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring HTTP Header Enrichment on page 135• tag (HTTP Header Enrichment) on page 742

term (HTTP Header Enrichment)

```
Syntax  term term-name {
        from {
            destination-address {
                (any-unicast | any-unicast except);
                [prefix];
            }
            destination-address-range {
                [high address low address] [except];
            }
            destination-port-range {
                [high port-number low port-number];
            }
            destination-ports [value];
            destination-prefix-list {
                (prefix-name | prefix-name except);
            }
        }
        then{
            count;
            tag tag-name {
                encrypt {
                    hash algorithm;
                    prefix hash-prefix;
                }
                tag-attribute tag-attr-name;
                tag-header header;
                tag-separator separator;
            }
        }
    }
```

Hierarchy Level [edit services hcm tag-rule *rule-name*]

Release Information Statement introduced in Junos OS Mobility Release 11.4W.

Description Configure the term (for the tag rule) that can be used to determine which HTTP headers are enriched. Multiple terms can be configured for a tag rule. Terms are evaluated in the order they are configured for a tag rule. If a data packet matches the criteria in any of the terms, then the actions specified in the **then** statement are applied. The data packet must match all the match conditions specified in a **from** statement. Once a term matches for a data packet, however, further terms are not evaluated. If no terms match, then the HTTP header is not enriched.



NOTE: You must configure at least one term for the tag rule.

The remaining statements are explained separately.

Options *term-name*—Identifier for the term.

Range: 1 through 32,767

Required Privilege interface—To view this statement in the configuration.
Level interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring HTTP Header Enrichment on page 135](#)
- [tag-rule \(HTTP Header Enrichment\) on page 745](#)

then (HTTP Header Enrichment)

Syntax

```
then {  
    count;  
    tag tag-name {  
        encrypt {  
            hash algorithm;  
            prefix hash-prefix;  
        }  
        tag-attribute tag-attr-name;  
        tag-header header;  
        tag-separator separator;  
    }  
}
```

Hierarchy Level [edit services hcm tag-rule *rule-name* term *term-name*]

Release Information Statement introduced in Junos OS Mobility Release 11.4W.

Description Specify the actions to be taken if the criteria specified in the tag rule are matched. All the actions specified here are applied when the criteria match.



NOTE: You must configure this statement and include at least one action to be taken for the tag rule term.

The remaining statements are explained separately.

Required Privilege interface—To view this statement in the configuration.
Level interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring HTTP Header Enrichment on page 135](#)
- [hcm \(HTTP Header Enrichment\) on page 711](#)

verify-source-address (APN)

Syntax	<code>verify-source-address { disable; }</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the verification of the IP address of the user equipment (UE) for the access point name (APN). The broadband gateway checks whether the source IP address in the data transfer packets from the user equipment is the same address that has been allocated by the gateway.
Default	If this statement is not configured, then the source IP address of the user equipment is always verified by the broadband gateway.
Options	disable —Disable the verification of the source IP address of the user equipment. The broadband gateway does not verify the source IP address of the user equipment during data transfers.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• apns on page 691• Configuring General APN Parameters on the Broadband Gateway on page 109

visitor-profile

Syntax	<code>visitor-profile visitor-profile;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> charging], [edit unified-edge gateways sgw <i>gateway-name</i> charging global-profile]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging global-profile] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Specify the profile that should be used to charge visiting subscribers. If the profile-selection-order configuration indicates static , then this profile is used for visiting subscribers.



NOTE: The charging profile must already be configured on the broadband gateway.

The broadband gateway determines whether the subscriber is a visitor by using 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). If the subscriber's International Mobile Subscriber Identity (IMSI), MCC, and MNC do not belong to the PLMN to which both the GGSN or P-GW and the S-GW belong, then the subscriber is deemed a visitor and the **visitor-profile** is applied. If the **visitor-profile** is not configured, then the **default-profile**, if configured, is applied. If the **default-profile** is also not configured, then the subscriber session is created with no charging applied.

Options	<code>visitor-profile</code> —Name of the visitor profile.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 119• Configuring S-GW Global Charging Profiles and Selection Order on page 282• charging (APN) on page 695• charging-profiles on page 780• global-profile (Serving Gateway) on page 806

wait-accounting (APN)

Syntax	wait-accounting;
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the user equipment (UE) sessions to wait for the accounting response from the authentication, authorization, and accounting (AAA) server, before sending the Create Session Response or Create packet data protocol (PDP) Response to the Serving Gateway (S-GW) or the serving GPRS support node (SGSN).</p> <p>If the APN is enabled for AAA accounting, then the broadband gateway, which receives the Create Session Request or Create PDP Context Request message from the user equipment, sends an Accounting Start message containing the subscriber's Mobile Station ISDN (MSISDN) number and IP address to the AAA server. Typically, the gateway does not wait for the accounting response from the AAA server before sending the Create Session Response or Create PDP Context Response message.</p> <p>However, when wait-accounting is enabled, the gateway will send the Create Session Response or Create PDP Context Response message after it receives the Accounting Start Response message from the AAA server.</p>
Default	If you do not configure this statement, then the gateway does not wait for the accounting response from the AAA server before sending the Create Session Response or Create PDP Context Response message to the S-GW or SGSN.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • apns on page 691 • Configuring General APN Parameters on the Broadband Gateway on page 109

Service Selection Profiles Configuration Statements

apn-name (Service Selection Profiles)

Syntax	<code>apn-name <i>apn-name</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> service-selection-profiles profile <i>name</i> term <i>name</i> then]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Specify the access point name (APN) to be used for the subscriber's session.</p> <p>This configuration is applicable only when the APN specified in the Create Session Request message from the subscriber is virtual. The virtual APN in the Create Session Request message is mapped to the real APN that you specify here.</p>



.....

NOTE: The APN that you specify must be **real** and must be configured on the broadband gateway.

.....

Options	<code>apn-name</code> —Name of the real APN.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring APN Service Selection on a Broadband Gateway on page 123• then (Service Selection Profiles) on page 767

charging-characteristics (Service Selection Profiles)

Syntax	<code>charging-characteristics <i>charging-characteristics</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> service-selection-profiles profile <i>name</i> term <i>name</i> from]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the charging characteristics for rule matching. If the value of the charging characteristics information element (IE) in the Create Session Request or Create Packet Data Protocol (PDP) Context message matches the charging characteristics value specified here, then the actions specified for the service selection profile are performed.
Options	<i>charging-characteristics</i> —Charging characteristics to be used for rule matching.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring APN Service Selection on a Broadband Gateway on page 123• from (Service Selection Profiles) on page 756

from (Service Selection Profiles)

Syntax `from {
 charging-characteristics charging-characteristics;
 imei imei;
 imsi imsi;
 maximum-bearers maximum-bearers;
 msisdn msisdn;
 pdn-type (ipv4 | ipv4v6 | ipv6);
 peer peer;
 peer-routing-instance peer-routing-instance;
 }`

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name* service-selection-profiles profile *name* term *name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the match criteria for the service selection profile term.



.....
NOTE: For any term, the subscriber must match all the match conditions specified in a `from` statement. If you do not configure the `from` statement, then all subscribers are considered a match.
.....


The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.


Related Documentation

- [Configuring APN Service Selection on a Broadband Gateway on page 123](#)
- [term \(Service Selection Profiles\) on page 766](#)

imei (Service Selection Profiles)

Syntax	<code>imei <i>imei</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> service-selection-profiles profile <i>name</i> term <i>name</i> from]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the International Mobile Station Equipment Identity (IMEI) for rule matching. If the IMEI of the user equipment (UE) matches the IMEI specified here, then the actions specified for the service selection profile are performed.
	<div>  <p>NOTE: You can specify either the full IMEI or a prefix—that is, the first few digits of the IMEI.</p> </div>
Options	<i>imei</i> —IMEI to be used for rule matching.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring APN Service Selection on a Broadband Gateway on page 123 • from (Service Selection Profiles) on page 756


imsi (Service Selection Profiles)

Syntax	<code>imsi <i>imsi</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> service-selection-profiles profile <i>name</i> term <i>name</i> from]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the International Mobile Subscriber Identity (IMSI) for rule matching. If the IMSI of the user equipment (UE) matches the IMSI specified here, then the actions specified for the service selection profile are performed.
	<div><p>NOTE: You can specify either the full IMSI or a prefix—that is, the first few digits of the IMSI.</p></div>
Options	<i>imsi</i> —IMSI to be used for rule matching.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring APN Service Selection on a Broadband Gateway on page 123• from (Service Selection Profiles) on page 756

maximum-bearers (Service Selection Profiles)

Syntax	maximum-bearers <i>maximum-bearers</i> ;
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> service-selection-profiles profile <i>name</i> term <i>name</i> from]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the maximum number of bearers to be used for rule matching. The <i>maximum-bearers</i> that you specify is matched against the number of bearers in the broadband gateway. If the number of bearers in the broadband gateway (at the time when the rule matching is done) exceeds the value that you specify, then that is considered a match.
Options	<i>maximum-bearers</i> —Maximum number of bearers to be used for rule matching. Range: 1 through 10,000,000
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring APN Service Selection on a Broadband Gateway on page 123 • from (Service Selection Profiles) on page 756

msisdn (Service Selection Profiles)

Syntax	<code>msisdn <i>msisdn</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> service-selection-profiles profile <i>name</i> term <i>name</i> from]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the Mobile Station ISDN (MSISDN) number for rule matching. If the MSISDN of the user equipment (UE) matches the MSISDN number specified here, then the actions specified for the service selection profile are performed.
	<div><p>NOTE: You can specify either the full MSISDN number or a prefix—that is, the first few digits of the MSISDN number.</p></div>
Options	<i>msisdn</i> —MSISDN number to be used for rule matching.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring APN Service Selection on a Broadband Gateway on page 123• from (Service Selection Profiles) on page 756


pdn-type (Service Selection Profiles)

Syntax	<code>pdn-type (ipv4 ipv4v6 ipv6);</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> service-selection-profiles profile <i>name</i> term <i>name</i> from]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the type of Packet Data Network (PDN) for rule matching. If the type of PDN of the user equipment (UE) matches the type of PDN specified here, then the actions specified for the service selection profile are performed.
Options	<p><code>ipv4</code>—Match PDNs supporting only IPv4.</p> <p><code>ipv4v6</code>—Match PDNs supporting both IPv4 and IPv6.</p> <p><code>ipv6</code>—Match PDNs supporting only IPv6.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring APN Service Selection on a Broadband Gateway on page 123 • from (Service Selection Profiles) on page 756

peer (Service Selection Profiles)

Syntax	<code>peer <i>peer</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> service-selection-profiles profile <i>name</i> term <i>name</i> from]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the IP address of the peer for rule matching. If the IP address of the peer creating the session matches the IP address specified here, then the actions specified for the service selection profile are performed.
Options	<code>peer</code> —IP address to be used for rule matching.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring APN Service Selection on a Broadband Gateway on page 123 • from (Service Selection Profiles) on page 756

peer-routing-instance (Service Selection Profiles)

Syntax	<code>peer-routing-instance <i>peer-routing-instance</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> service-selection-profiles profile <i>name</i> term <i>name</i> from]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the peer routing instance for rule matching. If the routing instance of the peer creating the session matches the routing instance specified here, then the actions specified for the service selection profile are performed.
<div> NOTE: This statement should be configured along with the <code>peer</code> statement.</div>	
Options	<code>peer-routing-instance</code> —Peer routing instance to be used for rule matching.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring APN Service Selection on a Broadband Gateway on page 123• from (Service Selection Profiles) on page 756

profile (Service Selection Profiles)

Syntax	<pre> profile <i>name</i> { term <i>name</i> { from { charging-characteristics <i>charging-characteristics</i>; imei <i>imei</i>; imsi <i>imsi</i>; maximum-bearers <i>maximum-bearers</i>; msisdn <i>msisdn</i>; pdn-type (ipv4 ipv4v6 ipv6); peer <i>peer</i>; peer-routing-instance <i>peer-routing-instance</i>; } then { apn-name <i>apn-name</i>; redirect-peer <i>redirect-peer</i>; } } } </pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> service-selection-profiles]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the name of the service selection profile that can be used by the access point name (APN). Multiple profiles can be configured on the broadband gateway. For each APN, you can specify a service selection profile.</p> <p>The remaining statements are explained separately.</p>
Options	<p><i>name</i>—Name of the service selection profile.</p> <p>Syntax: Up to 63 characters.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring APN Service Selection on a Broadband Gateway on page 123 • service-selection-profiles on page 765

redirect-peer (Service Selection Profiles)

Syntax	<code>redirect-peer <i>redirect-peer</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> service-selection-profiles profile <i>name</i> term <i>name</i> then]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Specify the IP address of the peer to which the Create Session Request should be redirected. The Create Session Request message is then redirected to the IP address of the redirect peer that you specify.</p> <p>The Create Session Response from the redirect peer is received by the broadband gateway and forwarded to the originator of the request. However, since the Create Session Response message contains the address of the redirected peer, further requests for the subscriber are directly sent by the originator to the redirect peer.</p>
Options	<i>redirect-peer</i> —IP address of the peer to which the session creation request should be redirected.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring APN Service Selection on a Broadband Gateway on page 123• then (Service Selection Profiles) on page 767

service-selection-profiles

```
Syntax  service-selection-profiles {
        profile name {
            term name {
                from {
                    charging-characteristics charging-characteristics;
                    imei imei;
                    imsi imsi;
                    maximum-bearers maximum-bearers;
                    msisdn msisdn;
                    pdn-type (ipv4 | ipv4v6 | ipv6);
                    peer peer;
                    peer-routing-instance peer-routing-instance;
                }
                then {
                    apn-name apn-name;
                    redirect-peer redirect-peer;
                }
            }
        }
    }
```

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the access point name (APN) to be used for the subscriber, or the broadband gateway that will service the subscriber. Service selection profiles specify how services are applied to a subscriber. The selection criteria specify the set of subscribers for whom the service is applied.

Multiple terms can be configured in a 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. After 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.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring APN Service Selection on a Broadband Gateway on page 123](#)
- [Example: Configuring Broadband Gateway APNs on page 126](#)

term (Service Selection Profiles)

Syntax	<pre>term <i>name</i> { from { charging-characteristics <i>charging-characteristics</i>; imei <i>imei</i>; imsi <i>imsi</i>; maximum-bearers <i>maximum-bearers</i>; msisdn <i>msisdn</i>; pdn-type (ipv4 ipv4v6 ipv6); peer <i>peer</i>; peer-routing-instance <i>peer-routing-instance</i>; } then { apn-name <i>apn-name</i>; redirect-peer <i>redirect-peer</i>; } }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> service-selection-profiles profile <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the term for the service selection profile that can be used by the access point name (APN).</p> <p>Multiple terms can be configured for a service selection profile. If a subscriber matches any of the terms, then the service specified in the then statement is applied. The subscriber must match all the match conditions specified in a from statement. Once a term matches for a subscriber, however, further terms are not evaluated. If no terms match for a subscriber, then the default services associated with the particular APN are applied.</p> <p>The remaining statements are explained separately.</p>
Options	<p>name—Name of the selection term.</p> <p>Syntax: Up to 63 characters.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring APN Service Selection on a Broadband Gateway on page 123• profile (Service Selection Profiles) on page 763

then (Service Selection Profiles)

Syntax then {
 `apn-name` *apn-name*;
 `redirect-peer` *redirect-peer*;
 }

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name* service-selection-profiles profile *name* term *name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Specify the action to be taken if the criteria specified in the service selection profile statement are matched.



NOTE: This statement is mandatory even if you have not specified any match criteria. The absence of match criteria (from statement) indicates that all subscribers are matched and the specified action is taken.

The remaining statements are explained separately.

Required Privilege interface—To view this statement in the configuration.
Level interface-control—To add this statement to the configuration.

Related Documentation


- [Configuring APN Service Selection on a Broadband Gateway on page 123](#)
- [term \(Service Selection Profiles\) on page 766](#)

Charging Configuration Statements

cdr-aggregation-limit

Syntax	<code>cdr-aggregation-limit value;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways], [edit unified-edge gateways sgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Configure the maximum number of Charging Data Records (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 charging data function (CDF) to the charging gateway function (CGF) server, when the cdr-aggregation-limit or the mtu size is reached (whichever comes first). For efficient transmissions of DRT messages, you may want to set the cdr-aggregation-limit to the maximum value of 16.
Options	value —Number of CDRs that can be added to a DRT message. Range: 1 through 16 Default: 5
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • charging-gateways on page 779 • Configuring Transport Profiles on page 295 • Configuring Charging on page 279

cdr-profile

Syntax	<code>cdr-profile <i>profile-name</i>;</code>
Hierarchy Level	<p>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i>],</p> <p>[edit unified-edge gateways sgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i>]</p>
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W.</p> <p>Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i>] hierarchy level introduced in Junos OS Mobility Release 11.4W.</p>
Description	<p>Associate a Charging Data Record (CDR) profile with a charging profile. However, make sure this profile has been previously defined.</p> <p>When a subscriber session is created, the subscriber is bound to a charging profile and the CDR profile configuration associated with this profile determines the information (fields) that is included in the CDRs and is used for billing purposes.</p> <p>Any modification to the existing configuration of this attribute must be done only when the charging profile with which it is associated is under active maintenance mode. Use one of the following commands, as applicable, to bring the charging profile under maintenance mode:</p> <ul style="list-style-type: none"> For the gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW)—<code>set unified-edge gateways ggsn-pgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i> service-mode maintenance</code> For the Serving Gateway (S-GW)—<code>set unified-edge gateways sgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i> service-mode maintenance</code>
	<div>  <p>TIP: If the profile is not already defined, use the one of the following commands, as applicable, to define a new CDR profile:</p> <ul style="list-style-type: none"> GGSN or P-GW—<code>set unified-edge gateways ggsn-pgw <i>gateway-name</i> charging cdr-profiles <i>profile-name</i></code> S-GW—<code>set unified-edge gateways sgw <i>gateway-name</i> charging cdr-profiles <i>profile-name</i></code> </div>
Options	<i>profile-name</i> —Name of the CDR profile to be associated with the charging profile.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> charging-profiles on page 780 Configuring Charging Profiles on page 300

- [Configuring Charging on page 279](#)
- [Charging Profiles on page 277](#)

cdr-profiles

Syntax `cdr-profiles profile-name {
 description string;
 enable-reduced-partial-cdrs;
 exclude-ie-options {
 apn-ni;
 apn-selection-mode;
 cc-selection-mode;
 dynamic-address;
 list-of-service-data;
 list-of-traffic-volumes;
 lrsn;
 ms-time-zone;
 network-initiation;
 node-id;
 pdn-connection-id;
 pdppdn-type;
 pgw-address-used; # S-GW only
 pgw-plmn-identifier;
 rat-type;
 record-sequence-number;
 served-imeisv;
 served-msisdn;
 served-pdppdn-address;
 serving-node-plmn-identifier;
 sgw-change; # S-GW only
 start-time;
 stop-time;
 user-location-information;
 }
 }
 }`

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name* charging],
 [edit unified-edge gateways sgw *gateway-name* charging]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.
 Support at the [edit unified-edge gateways sgw *gateway-name* charging] hierarchy level
 introduced in Junos OS Mobility Release 11.4W.

Description Configure a Charging Data Record (CDR) profile. The configuration in the CDR profile
 determines the content or the information that is included in a CDR and is used for billing
 purposes.

By default, the Juniper Charging Service (J-CS) module adds all the required fields mandated by the Third-Generation Partnership Project (3GPP) standards to the CDR. However, you can exclude the provisional fields information from the CDR by configuring a CDR profile.

The maximum number of CDR profiles supported for the broadband gateway is 255.

The remaining statements are explained separately.

Options	<i>profile-name</i> —Name of the CDR profile. Values: 1 through 128 bytes
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • charging on page 775 • Configuring CDR Attributes on page 298 • Configuring Charging on page 279

cdr-release


Syntax	<code>cdr-release (r7 r8 r99);</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways], [edit unified-edge gateways sgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	The encoding of the Charging Data Record (CDR) is compliant with the 3GPP technical specification release version that is configured using the statement. The supported versions are 3GPP release versions 7, 8, and 99.



NOTE: 3GPP release versions 7 and 99 are not applicable to the Serving Gateway (S-GW). 3GPP release version 8 is applicable to the GGSN, P-GW, and S-GW.

Options	<p>r7—3GPP release version, 7.</p> <p>r8—3GPP release version, 8.</p> <p>r99—3GPP release version, 99.</p> <p>Default: r8</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • charging-gateways on page 779 • Configuring Transport Profiles on page 295 • Configuring Charging on page 279

cdrs-per-file

Syntax	<code>cdrs-per-file value;</code>
Hierarchy Level	<code>[edit unified-edge gateways ggsn-pgw gateway-name charging local-persistent-storage-options],</code> <code>[edit unified-edge gateways sgw gateway-name charging local-persistent-storage-options]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the <code>[edit unified-edge gateways sgw gateway-name charging local-persistent-storage-options]</code> hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the maximum number of Charging Data Records (CDRs) that can be added to a file after which the temporary CDR log file is closed and moved to a final location within the same disk (<code>/opt/mobility/charging/ggsn/final_log</code>), from where it can be transferred using SSH FTP (SFTP). Files transferred from the final location should be deleted from the local Routing Engine disk after the transfer. Only authorized users can transfer and delete the files (after the transfer).</p> <p>However, any one of the following conditions must be met (whichever comes first) before the files are moved from the temporary location to the final location:</p> <ul style="list-style-type: none">• Number of CDRs per file reaches the configured or default limit.• Size of the file reaches the configured or default limit.• Age of the file reaches the configured or default limit. <div><p>NOTE: The default limit is applicable only if you have not configured any value.</p></div>
Options	<p>value—Maximum number of CDRs that can be added to a file after which it is closed and moved to a location within the Routing Engine disk, from where it can be transferred using SFTP.</p> <p>Range: 5000 through 1,000,000</p> <p>Default: 0, which indicates that there is no trigger for the CDR count per file.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• local-persistent-storage-options on page 810• Configuring Persistent Storage on page 291• Configuring Charging on page 279

charging

```
Syntax  charging {
        cdr-profiles profile-name {
            description string;
            enable-reduced-partial-cdrs;
            exclude-ie-options {
                apn-ni;
                apn-selection-mode;
                cc-selection-mode;
                dynamic-address;
                list-of-service-data;
                list-of-traffic-volumes;
                lrsn;
                ms-time-zone;
                network-initiation;
                node-id;
                pdn-connection-id;
                pdppdn-type;
                pgw-address-used; # S-GW only
                pgw-plmn-identifier;
                rat-type;
                record-sequence-number;
                served-imeisv;
                served-msisd;
                served-pdppdn-address;
                serving-node-plmn-identifier;
                sgw-change; # S-GW only
                start-time;
                stop-time;
                user-location-information;
            }
        }
        charging-profiles profile-name {
            cdr-profile profile-name;
            default-rating-group rg-num;
            default-service-id id-num;
            description string;
            profile-id id-num;
            transport-profile profile-name;
            trigger-profile profile-name;
            service-mode maintenance;
        }
        global-profile { # S-GW only
            default-profile default-profile;
            home-profile home-profile;
            profile-selection-order [profile-selection-method];
            roamer-profile roamer-profile;
            visitor-profile visitor-profile;
        }
        gtp {
            destination-port port-number;
            down-detect-time duration;
            echo-interval duration;
        }
    }
```

```
header-type (long | short);
n3-requests requests;
no-path-management;
pending-queue-size value;
peer peer-name {
    destination-ipv4-address address;
    destination-port port-number;
    down-detect-time duration;
    echo-interval duration;
    header-type (long | short);
    n3-requests requests;
    no-path-management;
    pending-queue-size value;
    reconnect-time duration;
    source-interface interface-name [ipv4-address address];
    t3-response response-interval;
    transport-protocol (tcp | udp);
    version (v0 | v1 | v2);
}
reconnect-time duration;
source-interface {
    interface-name;
    ipv4-address address;
}
t3-response response-interval;
transport-protocol (tcp | udp);
version (v0 | v1 | v2);
}
local-persistent-storage-options {
    cdrs-per-file value;
    disable-replication;
    disk-space-policy {
        watermark-level-1 {
            notification-level (both | snmp-alarm | syslog);
            percentage value;
        }
        watermark-level-2 {
            notification-level (both | snmp-alarm | syslog);
            percentage value;
        }
        watermark-level-3 {
            notification-level (both | snmp-alarm | syslog);
            percentage value;
        }
    }
}
file-age value;
file-creation-policy (shared-file | unique-file);
file-format (3gpp | raw-asn);
file-name-private-extension string;
file-size value;
traceoptions {
    file file-name <files number> <match regular-expression> <no-world-readable |
        world-readable> <size size>;
    flag flag;
    level (all | critical | error | info | notice | verbose | warning);
    no-remote-trace;
```

```

    }
    user-name string;
    world-readable;
  }
  traceoptions {
    file file-name <files number> <no-world-readable | world-readable> <size size>;
    flag flag;
    level (all | critical | error | info | notice | verbose | warning);
    no-remote-trace;
  }
  transport-profiles profile-name {
    description string;
    offline {
      charging-gateways {
        cdr-aggregation-limit value;
        cdr-release (r7 | r8 | r99);
        mtu value;
        peer-order {
          [peer charging-gateway-peer-name];
        }
        persistent-storage-order {
          local-storage;
        }
        switch-back-time seconds;
      }
    }
    service-mode maintenance;
  }
  trigger-profiles profile-name {
    description string;
    offline {
      container-limit value;
      exclude {
        ms-timezone-change;
        plmn-change;
        qos-change;
        rat-change;
        sgsn-mme-change; #S-GW only
        sgsn-sgw-change; #P-GW only
        user-location-change;
      }
      sgsn-mme-change-limit value; #S-GW only
      sgsn-sgw-change-limit value; #P-GW only
      time-limit value;
      volume-limit {
        value;
        direction (both | uplink);
      }
    }
    tariff-time-list {
      [tariff-time];
    }
  }
}

```

Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i>], [edit unified-edge gateways sgw <i>gateway-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i>] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>The configuration in this hierarchy determines the overall charging configuration for a subscriber.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• ggsn-pgw on page 986• Configuring Charging on page 279• Charging on page 271• Charging Services Overview on page 271• Charging Data Records on page 273• Charging Profiles on page 277• sgw on page 998

charging-gateways

Syntax	<pre> charging-gateways { cdr-aggregation-limit value; cdr-release (r7 r8 r99); mtu value; peer-order { [peer charging-gateway-peer-name]; } persistent-storage-order { local-storage; } switch-back-time seconds; } </pre>
Hierarchy Level	<p>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline],</p> <p>[edit unified-edge gateways sgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline]</p>
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W.</p> <p>Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline] hierarchy level introduced in Junos OS Mobility Release 11.4W.</p>
Description	<p>Configure a group of GTP Prime peers, the local Routing Engine disk, or both for Charging Data Record (CDR) file storage. In addition, you can configure the following:</p> <ul style="list-style-type: none"> • The maximum CDRs that can be added to a Data Record Transfer (DRT) message. • The maximum transmission unit of a DRT message. • The generated CDRs to be compliant with a specific 3GPP release. • The duration the charging data function (CDF) waits before transmitting the CDRs to a peer that has recently come up and has the highest priority among all the peers, which are alive. <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • offline on page 815 • Configuring Transport Profiles on page 295 • Configuring Charging on page 279

charging-profiles

Syntax	<pre>charging-profiles <i>profile-name</i> { <i>cdr-profile profile-name</i>; <i>default-rating-group rg-num</i>; <i>default-service-id id-num</i>; <i>description string</i>; <i>profile-id id-num</i>; <i>service-mode maintenance</i>; <i>transport-profile profile-name</i>; <i>trigger-profile profile-name</i>; }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging], [edit unified-edge gateways sgw <i>gateway-name</i> charging]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure a charging profile. The charging profile determines the overall charging configuration for a subscriber, such as the data collected in a Charging Data Record (CDR), the events that generate the CDR, where the CDR is stored, and so on for that subscriber.</p> <p>You can configure up to a maximum of 255 charging profiles.</p> <p>The remaining statements are explained separately.</p>
Options	<p><i>profile-name</i>—Name of the charging profile.</p> <p>Values: 1 through 128 bytes</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• charging on page 775• Configuring Charging Profiles on page 300• Charging Profiles on page 277• Configuring Charging on page 279

container-limit

Syntax	container-limit <i>value</i> ;
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i> offline], [edit unified-edge gateways sgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i> offline]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i> offline] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Configure the maximum number of containers that can be added to a Charging Data Record (CDR). When the limit is reached, the CDR is closed.
Options	value —Maximum number of containers. Range: 1 through 15 Default: 5
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • offline on page 816 • Configuring Charging Trigger Events on page 296 • Configuring Charging on page 279

default-profile

Syntax	<code>default-profile <i>default-profile</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> charging], [edit unified-edge gateways sgw <i>gateway-name</i> charging global-profile]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging global-profile] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Specify the default profile. If the profile-selection-order configuration indicates 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.




NOTE: The charging profile must already be configured on the broadband gateway.


The broadband gateway determines the type of subscriber by using 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) and compares these with the corresponding values configured for the home public land mobile network (HPLMN). Depending on whether a subscriber is a home subscriber, a visitor, or a roamer, the **home-profile**, **visited-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 also not configured, then the subscriber session is created with no charging applied.

Options	<i>default-profile</i> —Name of the default profile.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 119• Configuring S-GW Global Charging Profiles and Selection Order on page 282• charging (APN) on page 695• charging-profiles on page 780• global-profile (Serving Gateway) on page 806

default-rating-group

Syntax	<code>default-rating-group <i>rg-num</i>;</code>
Hierarchy Level	<p>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i>],</p> <p>[edit unified-edge gateways sgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i>]</p>
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W.</p> <p>Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i>] hierarchy level introduced in Junos OS Mobility Release 11.4W.</p>
Description	<p>Specify a default rating group to be used for charging service data containers. The rating group represents a collection of services.</p> <p>When this option is configured and if the Charging Data Record (CDR) release used is r7, then the P-GW generates a service data container, which is added to the CDR.</p>
	<div>  <p>NOTE: This configuration is not applicable for the Serving Gateway (S-GW).</p> </div>
Options	<i>rg-num</i> —Default rating group to be used for charging.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • charging-profiles on page 780 • Configuring Charging Profiles on page 300 • Charging Profiles on page 277 • Configuring Charging on page 279

default-service-id

Syntax	default-service-id <i>id-num</i> ;
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i>], [edit unified-edge gateways sgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i>] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Specify the default service identifier to be used for charging service data containers. This ID is used to identify the service or the service component.</p> <p>When this option is configured and if the Charging Data Record (CDR) release used is r7, then the P-GW generates a service data container, which is added to the CDR.</p>
<div> NOTE: This configuration is not applicable for the Serving Gateway (S-GW).</div>	
Options	<i>id-num</i> —Default service identifier to be used for charging.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• charging-profiles on page 780• Configuring Charging Profiles on page 300• Charging Profiles on page 277• Configuring Charging on page 279

description

Syntax	<code>description string;</code>
Hierarchy Level	<p>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging cdr-profiles <i>profile-name</i>], [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i>], [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i>], [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i>], [edit unified-edge gateways sgw <i>gateway-name</i> charging cdr-profiles <i>profile-name</i>], [edit unified-edge gateways sgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i>], [edit unified-edge gateways sgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i>], [edit unified-edge gateways sgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i>]</p>
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W.</p> <p>Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging cdr-profiles <i>profile-name</i>], [edit unified-edge gateways sgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i>], [edit unified-edge gateways sgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i>], and [edit unified-edge gateways sgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i>] hierarchy levels introduced in Junos OS Mobility Release 11.4W.</p>
Description	<p>Enter a description for the Charging Data Record (CDR) profile, charging profile, transport profile, or trigger profile (which can be used to capture the purpose of the profile). For example, you might have a description to differentiate the default profile from other profiles, as follows:</p> <p>This is the default profile to be used when a subscriber cannot be categorized into any other profile.</p> <p>However, make sure that the description is 255 characters or fewer.</p>
Options	<p>string—Description of the profile.</p> <p>Values: Up to 255 characters</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • cdr-profiles on page 772 • charging-profiles on page 780 • transport-profiles on page 843 • trigger-profiles on page 846 • Configuring CDR Attributes on page 298 • Configuring Charging Profiles on page 300 • Configuring Transport Profiles on page 295 • Configuring Charging Trigger Events on page 296

destination-ipv4-address (GTP Prime)

Syntax	<code>destination-ipv4-address <i>address</i>;</code>
Hierarchy Level	[edit unified-edge gateways <i>ggsn-pgw gateway-name</i> charging gtp peer <i>peer-name</i>], [edit unified-edge gateways <i>sgw gateway-name</i> charging gtp peer <i>peer-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways <i>sgw gateway-name</i> charging gtp peer <i>peer-name</i>] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Configure the charging gateway function (CGF) server's (GTP Prime peer's) IPv4 address, to which the Charging Data Records (CDRs) are sent as GTP Prime messages from the charging gateway function (CGF). This is a mandatory configuration.
Options	<i>address</i> —IPv4 address of the CGF server.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• peer (GTP Prime) on page 817• Configuring GTP Prime Peers on page 290• Configuring GTP Prime for Charging on page 289

destination-port (GTP Prime)

Syntax	<code>destination-port <i>port-number</i>;</code>
Hierarchy Level	<p>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging gtp],</p> <p>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>],</p> <p>[edit unified-edge gateways sgw <i>gateway-name</i> charging gtp],</p> <p>[edit unified-edge gateways sgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>]</p>
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W.</p> <p>Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging gtp] and [edit unified-edge gateways sgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>] hierarchy levels introduced in Junos OS Mobility Release 11.4W.</p>
Description	<p>Configure the TCP or UDP port on which the charging gateway function (CGF) server listens to the GTP Prime messages sent from the charging data function (CDF).</p> <p>When there are global-level and peer-level configurations, the peer-level configuration takes precedence.</p>
Options	<p><i>port-number</i>—TCP or UDP port on which the CGF server listens to the GTP Prime messages sent from the CDF.</p> <p>Range: 1 through 65535</p> <p>Default: 3386</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • gtp on page 807 • peer (GTP Prime) on page 817 • Configuring GTP Prime Peers on page 290 • Configuring GTP Prime for Charging on page 289

direction (Trigger Profiles)

Syntax	direction (both uplink);
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i> offline volume-limit], [edit unified-edge gateways sgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i> offline volume-limit]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i> offline volume-limit] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Specify whether the maximum volume of data transmitted includes the data transmitted in both the uplink and downlink directions, or only in the uplink direction.</p> <p>When the configured volume limit is reached, the CDR is updated with the transmitted uplink and downlink bytes and is closed.</p> <p>Any change to the existing configuration does not affect a previously established session. The updated configuration applies only to new sessions.</p>
Default	If you do not configure the direction statement, then the configured volume limit includes the total volume of data transmitted in both uplink and downlink directions.
Options	<p>both—The configured volume limit must include the total volume of data transmitted in both uplink and downlink directions.</p> <p>uplink—The configured volume limit must include the volume of data transmitted only in the uplink direction.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• volume-limit on page 850• Configuring Charging Trigger Events on page 296• Configuring Charging on page 279

disable-replication

Syntax	disable-replication;
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging local-persistent-storage-options], [edit unified-edge gateways sgw <i>gateway-name</i> charging local-persistent-storage-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging local-persistent-storage-options] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Specify that Charging Data Records (CDRs) stored on the Routing Engine disk should <i>not</i> be replicated to the standby Routing Engine. Typically, the CDRs stored on Routing Engine disk are replicated to the standby Routing Engine, as a backup. By default, replication is enabled.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • local-persistent-storage-options on page 810 • Configuring Persistent Storage on page 291 • Configuring Charging on page 279

disk-space-policy

Syntax	<pre>disk-space-policy { watermark-level-1 { notification-level (both snmp-alarm syslog); percentage <i>value</i>; } watermark-level-2 { notification-level (both snmp-alarm syslog); percentage <i>value</i>; } watermark-level-3 { notification-level (both snmp-alarm syslog); percentage <i>value</i>; } }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging local-persistent-storage-options], [edit unified-edge gateways sgw <i>gateway-name</i> charging local-persistent-storage-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging local-persistent-storage-options] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>When you use the Routing Engine disk to store Charging Data Records (CDRs), you may want to monitor and raise alerts if the disk space falls below a configured threshold level, which enables you to take appropriate measures to prevent the loss of CDR data.</p> <p>Use the statements within this hierarchy to configure the percentage of disk space you want to allocate for storage, and raise alerts when the limit is reached.</p> <p>You can configure up to a maximum of three threshold levels.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• local-persistent-storage-options on page 810• Configuring Persistent Storage on page 291• Configuring Charging on page 279

down-detect-time (GTP Prime)

Syntax	<code>down-detect-time <i>duration</i>;</code>
Hierarchy Level	<p>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging gtp],</p> <p>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>],</p> <p>[edit unified-edge gateways sgw <i>gateway-name</i> charging gtp],</p> <p>[edit unified-edge gateways sgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>]</p>
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W.</p> <p>Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging gtp] and [edit unified-edge gateways sgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>] hierarchy levels introduced in Junos OS Mobility Release 11.4W.</p>
Description	<p>Configure the duration for which the charging data function (CDF) must wait for a response from the charging gateway function (CGF) server after the expiry of an $n3 * t3$ cycle, after which the server's status is marked Down. The CDF then sends the GTP Prime messages to the next configured CGF server in the corresponding transport profile.</p> <p>When there are global-level and peer-level configurations, the peer-level configuration takes precedence.</p>
Options	<p><i>duration</i>—Duration the CDF waits after the $n3 * t3$ cycle expiry before declaring a GTP Prime peer as Down. The CDF then sends the GTP Prime messages to the next configured GTP Prime peer in the corresponding transport profile.</p> <p>Range: 0 through 255 seconds</p> <p>Default: 10 seconds</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • gtp on page 807 • peer (GTP Prime) on page 817 • Configuring GTP Prime Peers on page 290 • Configuring GTP Prime for Charging on page 289 • Configuring Charging on page 279

echo-interval (GTP Prime)

Syntax	<code>echo-interval <i>duration</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging gtp], [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>], [edit unified-edge gateways sgw <i>gateway-name</i> charging gtp], [edit unified-edge gateways sgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging gtp] and [edit unified-edge gateways sgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>] hierarchy levels introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the number of seconds that the charging data function (CDF) must wait before sending an echo request message to the charging gateway function (CGF) server.</p> <p>Echo messages are:</p> <ul style="list-style-type: none">• Sent only for UDP connections.• Not sent more than once in a minute. <p>When there are global-level and peer-level configurations, the peer-level configuration takes precedence.</p>
Options	<p><i>duration</i>—Number of seconds that the CDF waits before sending an echo request message to the CGF server.</p> <p>Range: 60 through 255 seconds</p> <p>Default: 60 seconds</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• gtp on page 807• peer on page 817• Configuring GTP Prime Peers on page 290• Configuring GTP Prime for Charging on page 289• Configuring Charging on page 279

enable-reduced-partial-cdrs

Syntax	enable-reduced-partial-cdrs;
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging cdr-profiles <i>profile-name</i>], [edit unified-edge gateways sgw <i>gateway-name</i> charging cdr-profiles <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging cdr-profiles <i>profile-name</i>] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Enable the generation of reduced partial Charging Data Records (RPCs). RPCs contain mandatory fields as well as information regarding changes in the session parameters relative to the previous CDR. For example, if the user equipment location has not changed, then this information is excluded from the RPC because this information has not changed from the previous CDR.
Default	If this statement is not configured, the generation of fully qualified partial CDR (FQPC) is supported. FQPC contains all the mandatory and conditional fields, as well as those fields that the public land mobile network (PLMN) operator has provisioned to be included in the CDR.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • cdr-profiles on page 772 • Configuring CDR Attributes on page 298 • Configuring Charging on page 279

exclude (Trigger Profiles)

Syntax	<pre>exclude { ms-timezone-change; plmn-change; qos-change; rat-change; sgsn-mme-change; #S-GW only sgsn-sgw-change; #P-GW only user-location-change; }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i> offline], [edit unified-edge gateways sgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i> offline]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i> offline] hierarchy level and the sgsn-mme-change option introduced in Junos OS Mobility Release 11.4W.
Description	<p>Certain signal message updates to the packet data protocol (PDP) context or bearer trigger charging updates. However, using the statements in this hierarchy, you can choose not to record these updates in the Charging Data Record (CDR).</p> <p>For example, a quality-of-service (QoS) change results in a container being added to the CDR. However, the container is not added if you configure to ignore this change, using one of the following commands, as applicable:</p> <ul style="list-style-type: none">• set unified-edge gateways ggsn-pgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i> exclude qos-change for the gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW).• set unified-edge gateways sgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i> exclude qos-change for the Serving Gateway (S-GW). <p>You may have configured certain information elements (IEs) to be excluded from the CDR using the statements at the [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging cdr-profiles <i>profile-name</i> exclude-ie-options] or the [edit unified-edge gateways sgw <i>gateway-name</i> charging cdr-profiles <i>profile-name</i> exclude-ie-options] hierarchy levels. Irrespective of this configuration, some of the IEs are to the CDR if the corresponding triggering event is not disabled. The following table lists the triggers and the corresponding IEs.</p>

Table 55: Triggers and Corresponding IEs

Trigger	IE
ms-timezone-change	Mobile Station (MS) time zone
plmn-change	Serving node PLMN identifier
rat-change	RAT type
user-location-change	User location information

Options



NOTE: The following options are applicable to both GGSN or P-GW and S-GW CDRs unless otherwise specified.

- **ms-timezone-change**—If configured, excludes charging data updates to the CDR when there is a change in the MS time zone. Otherwise, when an MS time zone change occurs, the CDR is updated with the charging information and is closed.
- **plmn-change**—If configured, excludes charging data updates to the CDR when there is a PLMN change. Otherwise, when a public land mobile network (PLMN) change occurs, the CDR is updated with the charging information and is closed.
- **qos-change**—If configured, excludes charging data updates to the CDR when there is a QoS change. Otherwise, a container is added to the CDR when there is a QoS change.
- **rat-change**—If configured, excludes charging data updates to the CDR when there is a RAT change. Otherwise, when a Radio Access Technology (RAT) change occurs, the CDR is updated with the charging information and is closed.
- **sgsn-mme-change**—(S-GW only) If configured, excludes charging data updates to the CDR when the SGSN or Mobility Management Entity (MME) changes reach the maximum configured limit (determined by the value set for the **sgsn-mme-change-limit** parameter). Otherwise, when the SGSN or MME changes reach the maximum configured limit, the CDR is updated and closed.
- **sgsn-sgw-change**—(GGSN or P-GW only) If configured, excludes charging data updates to the CDR when the SGSN or S-GW changes reach the maximum configuration limit (determined by the value set for the **sgsn-sgw-change-limit** parameter). Otherwise, when the SGSN or S-GW changes reach the maximum configured limit, the CDR is updated and closed.
- **user-location-change**—If configured, excludes charging data updates to the CDR when there is a change in user location. Otherwise, when a change in the user location information (such as E-UTRAN cell global identifier [ECGI], Tracking Area Identity [TAI], Routing Area Identity [RAI], SAI [Service Area identity], Location Area Identity [LAI], or Cell Global Identity [CGI]) occurs, the open containers are closed and added to the CDR.

Required Privilege interface—To view this statement in the configuration.
Level interface-control—To add this statement to the configuration.

Related Documentation

- [offline on page 816](#)
- [Configuring Charging Trigger Events on page 296](#)
- [Configuring Charging on page 279](#)

exclude-ie-options

Syntax	<pre> exclude-ie-options { apn-ni; apn-selection-mode; cc-selection-mode; dynamic-address; list-of-service-data; list-of-traffic-volumes; lrsn; ms-time-zone; network-initiation; node-id; pdn-connection-id; pdppdn-type; pgw-address-used; # S-GW only pgw-plmn-identifier; rat-type; record-sequence-number; served-imeisv; served-msisdn; served-pdppdn-address; serving-node-plmn-identifier; sgw-change; # S-GW only start-time; stop-time; user-location-information; } </pre>
Hierarchy Level	<p>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging cdr-profiles <i>profile-name</i>],</p> <p>[edit unified-edge gateways sgw <i>gateway-name</i> charging cdr-profiles <i>profile-name</i>]</p>
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W.</p> <p>pgw-address-used and sgw-change options and support for them at the [edit unified-edge gateways sgw <i>gateway-name</i> charging cdr-profiles <i>profile-name</i>] hierarchy level introduced in Junos OS Mobility Release 11.4W.</p>
Description	<p>The mobile operator can provision certain optional information elements (parameters) to be excluded from the Charging Data Record (CDR). Use this statement to configure the information elements (IEs) that are to be excluded from the CDR. By default, all informational elements are included in the CDR.</p>



CAUTION: Some of the IEs are added to the CDR irrespective of whether or not you have configured them to be excluded, if the corresponding triggering events are enabled. The **ms-time-zone**, **serving-node-plmn-identifier**, **rat-type**, and **user-location-information** IEs are added to the CDR, unless the corresponding **ms-timezone-change**, **plmn-change**, **rat-change**, and **user-location-change** triggering events are explicitly disabled using the statements under the **trigger-profiles > exclude** hierarchy level.

Options



NOTE: The following options are applicable to both the gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW) and Serving Gateway (S-GW) CDRs unless otherwise specified.

- **apn-ni**—The Access Point Name Network Identifier (APN-NI) defines the external network to which the user wants to connect to through the GGSN.
 - **apn-selection-mode**—Indicates the origin of the APN and whether or not the Home Location Register (HLR) or Home Subscriber Server (HSS) has verified the user's subscription. The possible values for this mode are:
 - **Mobile Station**—MS-provided APN, subscription not verified.
Indicates that the Mobile Station (MS) provided the APN and that the HLR or HSS did not verify the user's subscription to the network.
 - **Network**—Network-provided APN, subscription not verified.
Indicates that the network provided a default APN because the MS did not provide an APN, and that the HLR or HSS did not verify the user's subscription to the network.
 - **Verified**—MS or network-provided APN, subscription verified.
Indicates that the MS or the network provided the APN and that the HLR or HSS verified the user's subscription to the network.
 - **cc-selection-mode**—Indicates the type of charging characteristic that the GGSN or P-GW applies to the CDR: **Home**, **Visiting**, **Roaming**, or **SGSN/S-GW supplied**.
 - **dynamic-address**—This field, if present in the CDR, indicates that the packet data protocol (PDP) address has been dynamically allocated for the specific PDP context.
 - **list-of-service-data**—This list includes one or more containers and each of the container includes a list of fields which records information about the volume of data transmitted in bytes in the uplink and downlink directions, quality-of-service (QoS) changes, and so on. For the complete list, refer to the 3GPP 32.298 v 8.7.0 technical specification.
 - **list-of-traffic-volumes**—This list includes one or more containers and each container includes a list of fields which records information about the volume of data transmitted, in bytes, in the uplink and downlink directions, the reason for closing the container, when the container is closed, and the location of the user equipment when this data transmission occurs.
- This IE element is applicable for CDRs that are compliant with the 3GPP R7 and R99 release specifications, only.
- **lrsn**—The Local Record Sequence Number (LRSN) is a unique and sequential number generated by the network node (GGSN or P-GW) and is assigned to the CDRs for tracking any missing billing records.
 - **ms-time-zone**—Mobile Station (MS) time zone.

This IE is added to the CDR, irrespective of whether or not you have configured it to be excluded, if the **ms-timezone-change** triggering event is enabled. See [exclude](#) to disable this triggering event.

This IE is applicable for CDRs that are compliant with the 3GPP R7 and R8 release specifications, only.

- **network-initiation**—This field, if present in the CDR, indicates that the PDP context is network initiated.

This information element is applicable for CDRs that are compliant with the 3GPP R7 and R99 release specifications, only.

- **node-id**—ID of the network element node that generates the CDR.

In the MX Series router, the node-id is *ggsn/pgw-ip-address:virtual-spic-id*.

- **pdn-connection-id**—This ID uniquely identifies different records belonging to the same Packet Data Network (PDN) connection. This field includes the charging ID of the first IP-CAN bearer activated within the PDN connection. Together with the P-GW address, it uniquely identifies the PDN connection.

This information element is applicable for CDRs that are compliant with the 3GPP R8 release specification, only.

- **pdppdn-type**—Both PDP Type and PDN Type define the end-user protocol used between the external PDN and the MS.

This information element is applicable for CDRs that are compliant with the 3GPP R8 release specification, only.

- **pgw-address-used**—Exclude the P-GW address-used IE from the CDR. This option is applicable only to the S-GW.

- **pgw-plmn-identifier**—P-GW PLMN identifier (mobile country code and mobile network code).

This information element is applicable for CDRs that are compliant with the 3GPP R8 and R99 release specifications, only.

- **rat-type**—The Radio Access Technology (RAT) type used by the MS: eUTRAN, GERAN, WLAN, GAN, HSPA Evolution, or evolved High Rate Packet Data (eHRPD).

This IE is added to the CDR, irrespective of whether or not you have configured it to be excluded, if the **rat-change** triggering event is enabled. See [exclude](#) to disable this triggering event.

This information element is applicable for CDRs that are compliant with the 3GPP R7 and R8 release specifications, only.

- **record-sequence-number**—A sequential number assigned to each partial CDR of a particular PDP context or IP-CAN bearer. This number is not assigned, if there is only one CDR generated during the lifetime of a subscriber.
- **served-imeisv**—The International Mobile Station Equipment Identity and Software Version Number (IMEISV) IE of the served mobile equipment (ME).
- **served-msisdn**—The MSISDN number of the served equipment.
- **served-pdppdn-address**—The served PDP context or IP-CAN bearer address IE.

- **serving-node-plmn-identifier**—The serving node (SGSN or S-GW) PLMN identifier (mobile country code and mobile network code).

This IE is added to the CDR, irrespective of whether or not you have configured it to be excluded, if the **plmn-change** triggering event is enabled. See [exclude](#) to disable this triggering event.

This information element is applicable for CDRs that are compliant with the 3GPP R8 release specification, only.

- **sgw-change**—Exclude the S-GW change IE from the CDR. This option is applicable only to the S-GW.
- **start-time**—Time when the IP-CAN session is established at the P-GW for the first bearer in this session.

This information element is applicable for CDRs that are compliant with the 3GPP R8 release specification, only.

- **stop-time**—Time when the user IP-CAN session is terminated for the last bearer in this session.

This information element is applicable for CDRs that are compliant with the 3GPP R8 release specification, only.


- **user-location-information**—The location of the user equipment during the service data container recording interval is excluded. If this IE is excluded from the container, then it is also excluded from the CDR.

This IE is added to the CDR, irrespective of whether or not you have configured it to be excluded, if the **user-location-change** triggering event is enabled. See [exclude](#) to disable this triggering event.

Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
---------------------------------	---

Related Documentation	<ul style="list-style-type: none">• cdr-profiles on page 772• Configuring CDR Attributes on page 298• Configuring Charging on page 279
------------------------------	--

file-age

Syntax	<code>file-age value;</code>
Hierarchy Level	<p>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging local-persistent-storage-options],</p> <p>[edit unified-edge gateways sgw <i>gateway-name</i> charging local-persistent-storage-options]</p>
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W.</p> <p>Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging local-persistent-storage-options] hierarchy level introduced in Junos OS Mobility Release 11.4W.</p>
Description	<p>Configure the duration, in minutes, after which the temporary Charging Data Record (CDR) log file is closed and moved to a final location within the same disk (<code>/opt/mobility/charging/ggsn/final_log</code>), from where it can be transferred using SSH FTP (SFTP). Files transferred from the final location should be deleted from the local Routing Engine disk after the transfer. Only authorized users can transfer and delete the files (after the transfer). However, any one of the following conditions must be met (whichever comes first) before the files are moved from the temporary location to the final location:</p> <ul style="list-style-type: none"> • The age of the file reaches the configured or default limit. • The size of the file reaches the configured or default limit. • The number of CDRs per file reaches the configured or default limit.
	<div>  <p>NOTE: The default limit is applicable only if you have not configured any value.</p> </div>
Options	<p>value—Duration, in minutes, after which a CDR file is closed and moved to a final location within the Routing Engine disk, from where it can be transferred using SFTP.</p> <p>Range: 60 through 7200 minutes</p> <p>Default: 120 minutes</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • local-persistent-storage-options on page 810 • Configuring Persistent Storage on page 291 • Configuring Charging on page 279

file-creation-policy

Syntax	<code>file-creation-policy (shared-file unique-file);</code>
Hierarchy Level	<code>[edit unified-edge gateways ggsn-pgw gateway-name charging local-persistent-storage-options],</code> <code>[edit unified-edge gateways sgw gateway-name charging local-persistent-storage-options]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the <code>[edit unified-edge gateways sgw gateway-name charging local-persistent-storage-options]</code> hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Configure whether Charging Data Records (CDRs) generated for a specific transport profile from all the services PICs should be routed to a single temporary file (shared-file option) or to multiple files, with each file storing CDRs generated from a single services PIC (unique-file configuration).
Default	If you do not include the file-creation-policy statement, CDRs from all the services PICs are routed to a single temporary file (shared-file option)
Options	<p>shared-file—CDRs are routed to the files based on the file-routing criteria of the transport profile. In this configuration, all the CDRs generated for a specific transport profile from all the services PICs are routed to a single CDR temporary file. When a file trigger, such as file size, file age, or CDR count, triggers temporary file closure, the files are moved to the final CDR location (<code>/opt/mobility/charging/ggsn/final_log</code>). This is the default.</p> <p>unique-file—CDRs are routed to the files based on the file routing criteria of the transport profile. In this configuration, all the CDRs generated for a specific transport profile from each services PIC are routed to a separate CDR temporary file. When a file trigger, such as file size, file age, or CDR count, triggers temporary file closure, the files are moved to a final CDR location (<code>/opt/mobility/charging/ggsn/final_log</code>).</p>
Required Privilege Level	<code>interface</code> —To view this statement in the configuration. <code>interface-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• local-persistent-storage-options on page 810• Configuring Persistent Storage on page 291• Configuring Charging on page 279

file-format

Syntax	<code>file-format (3gpp raw-asn);</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging local-persistent-storage-options], [edit unified-edge gateways sgw <i>gateway-name</i> charging local-persistent-storage-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging local-persistent-storage-options] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Specify the file format for Charging Data Records (CDRs) stored in the CDR log files.
Default	If you do not include the file-format statement, the CDRs are stored in a format compliant with the 3GPP 32297 technical specification release (3gpp option).
Options	3gpp —CDRs are stored in a format that is compliant with the 3GPP 32297 technical specification release. raw-asn —CDRs are stored in raw Abstract Syntax Notation One (ASN.1) format.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • local-persistent-storage-options on page 810 • Configuring Persistent Storage on page 291 • Configuring Charging on page 279

file-name-private-extension

Syntax	<code>file-name-private-extension <i>string</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging local-persistent-storage-options], [edit unified-edge gateways sgw <i>gateway-name</i> charging local-persistent-storage-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging local-persistent-storage-options] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Specify a private extension (string) that is appended to the filenames.



NOTE: The filenaming format is as follows, which is compliant with the Third-Generation Partnership Project (3GPP) 32.297 technical release specification:


NodeID_-RC.date_-_time[.PI][.FE]

- **NodeID**—Name of the host that generated the file (*Host_Name_Gateway_Name*).
- **RC**—A running counter, starting at 1.
- **date**—Date when the CDR file was closed in YYYYMMDD (year, month, day) format.
- **time**—Time when the CDR file was closed in HHMMshhmm format.
 - *HHMM* indicates the local time (hours and minutes) in a 24-hour format.
 - *s* indicates the sign of the local time differential from the UTC (+ or -). If the time differential to the UTC is 0, then the sign can be arbitrarily set to + or -.
 - *hhmm* indicates the time differential (hours and minutes) from the UTC.
- **PI**—Optional private extension.
- **FE**—Optional file extension.

Options	<i>string</i> —Private extension. Values: 1 through 16 bytes
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• local-persistent-storage-options on page 810

- [Configuring Persistent Storage on page 291](#)
- [Configuring Charging on page 279](#)

file-size

Syntax	<code>file-size value;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging local-persistent-storage-options], [edit unified-edge gateways sgw <i>gateway-name</i> charging local-persistent-storage-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging local-persistent-storage-options] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure maximum size that the file can reach, in MB, after which the temporary Charging Data Record (CDR) log file is closed and moved to a final location within the same disk (<code>/opt/mobility/charging/ggsn/final_log</code>), from where it can be transferred using SSH FTP (SFTP). Files transferred from the final location should be deleted from the local Routing Engine disk after the transfer. Only authorized users can transfer and delete the files (after the transfer). However, any one of the following conditions must be met (whichever comes first):</p> <ul style="list-style-type: none"> • Size of the file reaches the configured or default limit. • Age of the file reaches the configured or default limit. • Number of CDRs per file reaches the configured or default limit.
	<div>  <p>NOTE: The default limit is applicable only if you have not configured any value.</p> </div>
Options	<p>value—Maximum size that the CDR file can reach, in MB, after which it is closed and moved to a final location within the Routing Engine disk, from where it can be transferred using SFTP.</p> <p>Range: 1 MB to 1024 MB</p> <p>Default: 10 MB</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • local-persistent-storage-options on page 810 • Configuring Persistent Storage on page 291 • Configuring Charging on page 279

global-profile (Serving Gateway)

Syntax	<pre>global-profile { default-profile default-profile; home-profile home-profile; profile-selection-order [profile-selection-method]; roamer-profile roamer-profile; visitor-profile visitor-profile; }</pre>
Hierarchy Level	[edit unified-edge gateways sgw <i>gateway-name</i> charging]
Description	<p>Configure the global (charging) profiles that will be applicable for the Serving Gateway (S-GW). This is a mandatory configuration if you want to enable charging on the S-GW. Configuring the profile-selection-order statement is mandatory if the global-profile statement is configured.</p> <p>The S-GW determines the type of subscriber by using 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) and compares these with the corresponding values configured for the home public land mobile network (HPLMN). 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 default-profile is also not configured, then the subscriber session is created with no charging applied.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring S-GW Global Charging Profiles and Selection Order on page 282• charging on page 775

gtp

Syntax	<pre> gtp { destination-port <i>port-number</i>; down-detect-time <i>duration</i>; echo-interval <i>duration</i>; header-type (long short); n3-requests <i>requests</i>; no-path-management; pending-queue-size <i>value</i>; peer <i>peer-name</i> { destination-ipv4-address <i>address</i>; destination-port <i>port-number</i>; down-detect-time <i>duration</i>; echo-interval <i>duration</i>; header-type (long short); n3-requests <i>requests</i>; no-path-management; pending-queue-size <i>value</i>; reconnect-time <i>duration</i>; source-interface <i>interface-name</i> [ipv4-address <i>address</i>]; t3-response <i>response-interval</i>; transport-protocol (tcp udp); version (v0 v1 v2); } reconnect-time <i>duration</i>; source-interface { <i>interface-name</i>; [ipv4-address <i>address</i>; } t3-response <i>response-interval</i>; transport-protocol (tcp udp); version (v0 v1 v2); } </pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging], [edit unified-edge gateways sgw <i>gateway-name</i> charging]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>The statements in this hierarchy enable you to set global as well as unique configurations for the general packet radio service (GPRS) tunneling protocol Prime (GTP Prime) peers (Charging Gateway Function [CGF] servers). If no separate configuration is defined for a peer, then the global configurations apply for that peer.</p> <p>The charging data function (CDF) sends the Charging Data Records (CDRs) as GTP Prime messages to the GTP Prime peer, based on this configuration.</p> <p>The remaining statements are explained separately.</p>

Required Privilege interface—To view this statement in the configuration.
Level interface-control—To add this statement to the configuration.

Related Documentation

- [charging on page 775](#)
- [Configuring GTP Prime for Charging on page 289](#)
- [Configuring GTP Prime Peers on page 290](#)
- [Configuring Charging on page 279](#)

header-type (GTP Prime)

Syntax header-type (long | short);

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name* charging gtp],
[edit unified-edge gateways ggsn-pgw *gateway-name* charging gtp peer *peer-name*],
[edit unified-edge gateways sgw *gateway-name* charging gtp],
[edit unified-edge gateways sgw *gateway-name* charging gtp peer *peer-name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.
Support at the [edit unified-edge gateways sgw *gateway-name* charging gtp] and [edit unified-edge gateways sgw *gateway-name* charging gtp peer *peer-name*] hierarchy levels introduced in Junos OS Mobility Release 11.4W.

Description Configure the charging data function (CDF) GTP Prime message header length to match the version supported on the charging gateway function (CGF) server, which can be set to either short (6 bytes) or long (20 bytes). The **long** format is supported only in GTP Prime version 0. GTP Prime versions 1 and 2 support the **short** header length only.

When there are global-level and peer-level configurations, the peer-level configuration takes precedence.

Options **long**—CDF GTP Prime message header length is set to 20 bytes.
short—CDF GTP Prime message header length is set to 6 bytes.

Required Privilege interface—To view this statement in the configuration.
Level interface-control—To add this statement to the configuration.

Related Documentation

- [gtp on page 807](#)
- [peer \(GTP Prime\) on page 817](#)
- [Configuring GTP Prime for Charging on page 289](#)
- [Configuring GTP Prime Peers on page 290](#)
- [Configuring Charging on page 279](#)

home-profile

Syntax	<code>home-profile <i>home-profile</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> charging], [edit unified-edge gateways sgw <i>gateway-name</i> charging global-profile]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging global-profile] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Specify the profile that should be used to charge home subscribers. If the profile-selection-order configuration indicates static , then this profile is used for home subscribers.



NOTE: The charging profile must already be configured on the broadband gateway.

The broadband gateway determines whether the subscriber is a home subscriber by using 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). If the subscriber's International Mobile Subscriber Identity (IMSI), MCC, and MNC belong to the same PLMN to which both the GGSN or P-GW and the S-GW belong, then the subscriber is deemed a home subscriber and the **home-profile** is applied. If the **home-profile** is not configured, then the **default-profile**, if configured, is applied. If the **default-profile** is also not configured, then the subscriber session is created with no charging applied.

Options	<i>home-profile</i> —Name of the home profile.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 119 • Configuring S-GW Global Charging Profiles and Selection Order on page 282 • charging (APN) on page 695 • charging-profiles on page 780 • global-profile (Serving Gateway) on page 806

local-persistent-storage-options

Syntax local-persistent-storage-options {
 cdrs-per-file *value*;
 disable-replication;
 disk-space-policy {
 watermark-level-1 {
 notification-level (both | snmp-alarm | syslog);
 percentage *value*;
 }
 watermark-level-2 {
 notification-level (both | snmp-alarm | syslog);
 percentage *value*;
 }
 watermark-level-3 {
 notification-level (both | snmp-alarm | syslog);
 percentage *value*;
 }
 }
 file-age *value*;
 file-creation-policy (shared-file | unique-file);
 file-format (3gpp | raw-asn);
 file-name-private-extension *string*;
 file-size *value*;
 traceoptions {
 file *file-name* <files *number*> <match *regular-expression*> <no-world-readable |
 world-readable> <size *size*> ;
 flag *flag*;
 level (all | critical | error | info | notice | verbose | warning);
 no-remote-trace;
 }
 user-name *string*;
 world-readable;
 }

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name* charging],
 [edit unified-edge gateways sgw *gateway-name* charging]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.
 Support at the [edit unified-edge gateways sgw *gateway-name* charging] hierarchy level
 introduced in Junos OS Mobility Release 11.4W.

Description Configure the Charging Data Record (CDR) file storage options, which are measures to
 prevent loss of the CDR data.

You typically store the CDRs on the local Routing Engine disk when you do not have any external charging gateway function (CGF) servers configured to store them or when all the CGF servers are down.

When you choose to store the CDRs locally, the CDRs generated by the services PICs are routed to a file on the Routing Engine disk. Some of the options that can be configured include the following:

- Action to be taken when the disk space falls below the configured watermark level.
- Restricting access to the files to a specific user.
- File routing criteria—CDRs are routed to the files based on the file-routing criteria of the transport profile. Therefore, all CDRs generated for a given transport profile are saved in a specific CDR log file.

The remaining statements are explained separately.

Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • charging on page 775 • Configuring Persistent Storage on page 291 • Configuring Charging on page 279

local-storage

Syntax	local-storage;
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways persistent-storage-order], [edit unified-edge gateways sgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways persistent-storage-order]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways persistent-storage-order] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Configure the Routing Engine disk as backup storage for the Charging Data Records (CDRs) when the external storage resources (charging gateway function [CGF] servers) are down or if no external servers are configured.
Default	If you do not include the local-storage statement, the backup storage is disabled.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • persistent-storage-order on page 821 • Configuring Persistent Storage on page 291 • Configuring Charging on page 279

mtu (Transport Profiles)

Syntax	<code>mtu value;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways], [edit unified-edge gateways sgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the maximum transmission unit (MTU) for a Data Record Transfer (DRT) message, which represents the maximum size in bytes that a DRT message can reach before it is transmitted.</p> <p>A DRT message containing the Charging Data Records (CDRs) is transmitted from the charging data function (CDF) to the charging gateway function (CGF) server, when the cdr-aggregation-limit or the mtu size is reached (whichever comes first).</p>
Options	<p>value—Maximum size, in bytes, for a DRT message.</p> <p>Range: 300 through 8000 bytes</p> <p>Default: 1500 bytes</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• charging-gateways on page 779• Configuring Transport Profiles on page 295• Configuring Charging on page 279

n3-requests (GTP Prime)

Syntax	<code>n3-requests <i>requests</i>;</code>
Hierarchy Level	<p>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging gtp],</p> <p>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>],</p> <p>[edit unified-edge gateways sgw <i>gateway-name</i> charging gtp],</p> <p>[edit unified-edge gateways sgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>]</p>
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W.</p> <p>Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging gtp] and [edit unified-edge gateways sgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>] hierarchy levels introduced in Junos OS Mobility Release 11.4W.</p>
Description	<p>Configure the maximum number of times the charging data function (CDF) attempts to send echo request messages to the charging gateway function (CGF) server, after which the CDF waits for a configured duration (see down-detect-time) for any response before declaring the server as Down.</p> <p>The broadband gateway retransmits the requests to the UDP peers. However, for the TCP peers, the requests are retransmitted to a newer peer (when there is a switchover) or to the same peer (when it becomes alive after being Down).</p> <p>When there are global-level and peer-level configurations, the peer-level configuration takes precedence.</p>
Options	<p><i>requests</i>—Number of times that the CDF attempts to send a request to a CGF server after which the CDF waits for a configured duration (see down-detect-time) before declaring the server as Down.</p> <p>Range: 1 through 5</p> <p>Default: 3</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • gtp on page 807 • peer (GTP Prime) on page 817 • Configuring GTP Prime for Charging on page 289 • Configuring GTP Prime Peers on page 290 • Configuring Charging on page 279

no-path-management (GTP Prime)

Syntax	no-path-management;
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging gtp], [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>], [edit unified-edge gateways sgw <i>gateway-name</i> charging gtp], [edit unified-edge gateways sgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging gtp] and [edit unified-edge gateways sgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>] hierarchy levels introduced in Junos OS Mobility Release 11.4W.
Description	Use this statement to disable path management messages. If this statement is configured, no echo messages are sent. However, the router responds to any echo messages that are received.



NOTE:

- Path management refers to the exchange of echo messages between charging data function (CDF) and charging gateway function (CGF) servers (GTP Prime peers) to find out whether a CGF server is alive to process the GTP Prime messages sent from the CDF.
 - Echo messages are sent only for UDP connections.
-

When there are global-level and peer-level configurations, the peer-level configuration takes precedence.

Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
---------------------------------	---

Related Documentation	<ul style="list-style-type: none">• gtp on page 807• peer (GTP Prime) on page 817• Configuring GTP Prime for Charging on page 289• Configuring GTP Prime Peers on page 290• Configuring Charging on page 279
------------------------------	--

offline (Transport Profiles)

Syntax	<pre> offline { charging-gateways { cdr-aggregation-limit value; cdr-release (r7 r8 r99); mtu value; peer-order { [peer charging-gateway-peer-name]; } persistent-storage-order { local-storage; } switch-back-time seconds; } } </pre>
Hierarchy Level	<p>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i>],</p> <p>[edit unified-edge gateways sgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i>]</p>
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W.</p> <p>Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i>] hierarchy level introduced in Junos OS Mobility Release 11.4W.</p>
Description	<p>Configure the transport parameters for offline charging records, such as:</p> <ul style="list-style-type: none"> • The charging gateway peers that store the CDRs. • The maximum Charging Data Records (CDRs) that can be added to a Data Record Transfer (DRT) message. • The maximum transmission unit of a DRT message. • The generated CDRs to be compliant with a specific 3GPP release. • The duration that the charging data function (CDF) waits before transmitting the CDRs to a peer that has recently come up and has the highest priority among all the peers, which are alive. • Whether to use the local Routing Engine disk for CDR storage. <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • transport-profiles on page 843 • Configuring Transport Profiles on page 295 • Configuring Charging on page 279

offline (Trigger Profiles)

Syntax	<pre>offline { container-limit value; exclude { ms-timezone-change; plmn-change; qos-change; rat-change; sgsn-mme-change; #S-GW only sgsn-sgw-change; #P-GW only user-location-change; } sgsn-mme-change-limit value; #S-GW only sgsn-sgw-change-limit value; #P-GW only time-limit value; volume-limit { value; direction (both uplink); } }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i>], [edit unified-edge gateways sgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i>] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the attributes that trigger charging updates for offline charging records.</p> <p>For example, you can set the maximum duration that the Charging Data Record (CDR) can remain open (time-limit), maximum volume of data that can be transmitted before closing a CDR (volume-limit), maximum number of containers that can be added to a CDR, or maximum number of Serving Gateway (S-GW) or serving GPRS support node (SGSN) changes that can occur before the CDR is updated and closed.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• trigger-profiles on page 846• Configuring Charging Trigger Events on page 296• Configuring Charging on page 279


peer (GTP Prime)

Syntax	<pre> peer <i>peer-name</i> { destination-ipv4-address <i>address</i>; destination-port <i>port-number</i>; down-detect-time <i>duration</i>; echo-interval <i>duration</i>; header-type (long short); n3-requests <i>requests</i>; no-path-management; pending-queue-size <i>value</i>; reconnect-time <i>duration</i>; source-interface { interface-name; ipv4-address <i>address</i>; } t3-response <i>response-interval</i>; transport-protocol (tcp udp); version (v0 v1 v2); } </pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging gtp], [edit unified-edge gateways sgw <i>gateway-name</i> charging gtp]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging gtp] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure GTP Prime peers (charging gateway function [CGF] servers). You can configure up to a maximum of 24 peers. The charging data function (CDF) sends the Charging Data Records (CDRs) as GTP Prime messages to the GTP Prime peer, based on this configuration.</p> <p>When there are global-level and peer-level configurations, the peer-level configuration takes precedence.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • gtp on page 807 • Configuring GTP Prime Peers on page 290 • Configuring GTP Prime for Charging on page 289 • Configuring Charging on page 279

peer (Peer Order)

Syntax	<code>peer charging-gateway-peer-name;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways peer-order], [edit unified-edge gateways sgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways peer-order]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways peer-order] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the name of the charging gateway peer. However, make sure the peer that you specify here is previously configured for its IP address, name, and so on, using one of the following statements, as applicable. Otherwise, you will encounter a configuration error.</p> <ul style="list-style-type: none">• <code>set unified-edge gateways ggsn-pgw <i>gateway-name</i> charging gtp peer</code> for the gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW).• <code>set unified-edge gateways sgw <i>gateway-name</i> charging gtp peer</code> for the Serving Gateway (S-GW).
Options	<i>charging-gateway-peer-name</i> —Name of the charging gateway server.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• peer-order on page 819• Configuring GTP Prime Peers on page 290• Configuring GTP Prime for Charging on page 289• Configuring Charging on page 279

peer-order

Syntax	<pre>peer-order { [peer charging-gateway-peer-name]; }</pre>
Hierarchy Level	<p>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways],</p> <p>[edit unified-edge gateways sgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways]</p>
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W.</p> <p>Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways] hierarchy level introduced in Junos OS Mobility Release 11.4W.</p>
Description	<p>Configure the charging gateway function (CGF) servers. You can configure up to a maximum of three servers for a transport profile.</p> <p>When multiple CGF servers are available for storing Charging Data Records (CDRs), the charging data function (CDF) needs to identify the server to which to route the CDRs first. The peer order determines this hierarchy using which the CDF tries to send the CDRs to the server that comes first in this order. The peer that comes first in the order is treated as the highest-priority peer. At any given time, CDRs are sent to only one of the peers and not to all. If for any reason the first server goes down, the CDF tries to send the CDRs to the server that comes next in the order. However, if a higher-priority peer comes up, the CDRs are sent to this peer after a waiting period determined by the switch-back-time configuration.</p> <p>When required, the priority of any peer can be changed by using the configuration option to insert before or insert after the existing peers.</p> <div style="margin-top: 20px;">  <p>NOTE: If all the peers are Down and if you have configured the Routing Engine disk as the backup storage option, then the CDRs are routed to the Routing Engine disk. However, if one or multiple peers come alive, then CDF waits for the configured switch-back-time duration and routes the CDRs to the highest priority peer that is alive after this duration. The CDRs that were getting stored previously on the Routing Engine disk are not routed to the charging gateway (peer) and remain on the disk. You need to transfer the CDRs using SSS FTP (SFTP) from the following location on the disk: /opt/mobility/charging/ggsn/final_log.</p> </div>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>

The remaining statements are explained separately.

- Related Documentation**
- [charging-gateways on page 779](#)
 - [Configuring GTP Prime Peers on page 290](#)
 - [Configuring GTP Prime for Charging on page 289](#)
 - [Configuring Charging on page 279](#)


pending-queue-size (GTP Prime)

Syntax	<code>pending-queue-size <i>value</i>;</code>
Hierarchy Level	<code>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging gtp],</code> <code>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>],</code> <code>[edit unified-edge gateways sgw <i>gateway-name</i> charging gtp],</code> <code>[edit unified-edge gateways sgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the <code>[edit unified-edge gateways sgw <i>gateway-name</i> charging gtp]</code> and <code>[edit unified-edge gateways sgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>]</code> hierarchy levels introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the maximum number of Data Record Transfer (DRT) messages that can be sent by the charging data function (CDF) without an acknowledgement from the charging gateway function (CGF) server. When the limit is reached, CDF stops sending the messages to that CGF server.</p> <p>When there are global-level and peer-level configurations, the peer-level configuration takes precedence.</p>
Options	<p>value—Maximum number of DRT messages that can be queued without an acknowledgement from the CGF server.</p> <p>Range: 1 through 4096</p> <p>Default: 1024</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• gtp on page 807• peer (GTP Prime) on page 817• Configuring GTP Prime Peers on page 290• Configuring GTP Prime for Charging on page 289• Configuring Charging on page 279


persistent-storage-order

Syntax	<code>persistent-storage-order { local-storage; }</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways], [edit unified-edge gateways sgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the local storage of Charging Data Records (CDRs). You may want to store the CDRs on the local Routing Engine disk for one of the following reasons:</p> <ul style="list-style-type: none"> • When there are no charging gateway peers configured for a transport profile • When none of the primary, secondary, or tertiary charging gateway peers can be reached (that is, when they are down) <p>The remaining statement is explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • charging-gateways on page 779 • Configuring Transport Profiles on page 295 • Configuring Charging on page 279

profile-id

Syntax	<code>profile-id <i>id-num</i>;</code>
Hierarchy Level	<code>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i>],</code> <code>[edit unified-edge gateways sgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i>]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the <code>[edit unified-edge gateways sgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i>]</code> hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure a unique identifier to be associated with a charging profile. It can range from 1 through 255. This is a mandatory configuration.</p> <p>Based on the user subscription, the Serving Gateway (S-GW), serving GPRS support node (SGSN), or RADIUS server returns the charging profile (identified by the profile ID) that must be used for charging the mobile subscriber. If more than one server returns a profile ID, then the profile selection order configuration determines which server's profile ID must be given higher priority. This profile ID is then matched with the profile-id that you have configured to choose the correct charging profile for that subscriber. However, if a server returns an incorrect or unconfigured charging profile ID, the profile ID returned by the server, which is next in priority, is taken into consideration. If none of the profile IDs match, then charging is disabled for the customer.</p> <div><p>NOTE: The RADIUS server returns the profile-id as a four-byte hexadecimal value in the access accept message.</p></div>
Options	<i>id-num</i> —A unique number to be associated with a charging profile. Range: 1 through 65534
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• charging-profiles on page 780• Configuring Charging Profiles on page 300• Charging Profiles on page 277• Configuring Charging on page 279

profile-selection-order (Serving Gateway)

Syntax	<code>profile-selection-order [<i>profile-selection-method</i>];</code>
Hierarchy Level	[edit unified-edge gateways <i>sgw gateway-name</i> charging global-profile]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	<p>Specify the order of the methods used to select a charging profile applicable for a subscriber's session on the Serving Gateway (S-GW). You can specify a maximum of 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.</p> <p>For example, consider a scenario where the profile selection order is static, serving, and pgw-cg-addr. Since static is the first choice, the global (charging) profiles specified are used. If the global 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 ID 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 charging profile is selected based on the IP address of the charging gateway (CG) for the P-GW.</p>
	<div>  <p>NOTE: If the charging profile cannot be selected by any of the methods specified, then charging is disabled for that subscriber.</p> </div>
Options	<p><i>profile-selection-method</i>—One or more profile selection methods, listed in the order in which they should be tried. The method can be one or more of the following:</p> <ul style="list-style-type: none"> • pgw-cg-addr—Use the charging profile based on the on the IP address of the CG for the P-GW. • serving—Use the charging profile sent by the SGSN or the Serving Gateway (S-GW). • static—Use the charging profile configured locally for the S-GW.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring S-GW Global Charging Profiles and Selection Order on page 282 • global-profile (Serving Gateway) on page 806

reconnect-time (GTP Prime)

Syntax	<code>reconnect-time <i>duration</i>;</code>
Hierarchy Level	<code>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging gtp],</code> <code>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>],</code> <code>[edit unified-edge gateways sgw <i>gateway-name</i> charging gtp],</code> <code>[edit unified-edge gateways sgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the <code>[edit unified-edge gateways sgw <i>gateway-name</i> charging gtp]</code> and <code>[edit unified-edge gateways sgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>]</code> hierarchy levels introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the duration (in seconds) that the charging data function (CDF) must wait before trying to reconnect to a charging gateway function (CGF) server that was marked Down earlier.</p> <p>When there are global-level and peer-level configurations, the peer-level configuration takes precedence.</p>
Options	<p><i>duration</i>—Duration after which the CDF tries to reconnect to a CGF server that was previously down.</p> <p>Range: 60 through 255 seconds. Enter 0 if you do not want to attempt to reconnect to a peer.</p> <p>Default: 60 seconds</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• gtp on page 807• peer (GTP Prime) on page 817• Configuring GTP Prime Peers on page 290• Configuring GTP Prime for Charging on page 289• Configuring Charging on page 279

roamer-profile

Syntax	<code>roamer-profile <i>roamer-profile</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> charging], [edit unified-edge gateways sgw <i>gateway-name</i> charging global-profile]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging global-profile] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Configure the profile that should be used to charge roaming subscribers. If the profile-selection-order configuration indicates static , then this profile is used for roaming subscribers.



NOTE: The charging profile must already be configured on the broadband gateway.

The broadband gateway determines whether the subscriber is a roamer by using 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). If the subscriber's International Mobile Subscriber Identity (IMSI), MCC, and MNC belong to the same PLMN as the GGSN or P-GW, but the S-GW belongs to a different PLMN, then the subscriber is deemed a roamer and the **roamer-profile** is applied. If the **roamer-profile** is not configured, then the **default-profile**, if configured, is applied. If the **default-profile** is also not configured, then the subscriber session is created with no charging applied.

Options	<i>roamer-profile</i> —Name of the roamer profile.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 119 • Configuring S-GW Global Charging Profiles and Selection Order on page 282 • charging (APN) on page 695 • charging-profiles on page 780 • global-profile (Serving Gateway) on page 806

service-mode (Charging Profiles)

Syntax	<code>service-mode maintenance;</code>
Hierarchy Level	<code>[edit unified-edge gateways ggsn-pgw gateway-name charging charging-profiles profile-name],</code> <code>[edit unified-edge gateways sgw gateway-name charging charging-profiles profile-name]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the <code>[edit unified-edge gateways sgw gateway-name charging charging-profiles profile-name]</code> hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Place the respective charging profile under maintenance mode.</p> <p>When you have to make the following changes to the existing charging profile configuration, you must put the charging profile in maintenance mode:</p> <ul style="list-style-type: none">• Change the CDR profile, transport profile, or the trigger profile associated with this charging profile• Change the profile ID configuration• Delete the charging profile <p>In maintenance mode, no new subscribers are accepted for that charging profile. However, maintenance mode does not become active until no existing subscriber sessions are using that charging profile and all the corresponding CDRs have been flushed out. Unless the maintenance mode becomes active, you cannot modify the above-mentioned charging profile attributes or delete the charging profile. Use the following commands to help you with maintenance mode tasks:</p> <ul style="list-style-type: none">• To verify that the charging profile has entered active maintenance mode, use one of the following commands, as applicable:<ul style="list-style-type: none">• For the gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW)—<code>show unified-edge ggsn-pgw charging service-mode gateway gateway-name charging-profile profile-name</code>• For the Serving Gateway (S-GW)—<code>show unified-edge sgw charging service-mode gateway gateway-name charging-profile profile-name</code>• To verify that the subscriber count has reached zero, use one of the following commands, as applicable:<ul style="list-style-type: none">• For the GGSN or P-GW—<code>show unified-edge ggsn-pgw subscribers charging charging-profile profile-name gateway gateway-name</code>• For the S-GW—<code>show unified-edge sgw subscribers charging charging-profile profile-name gateway gateway-name</code>• To verify that all CDRs for the transport profile referred to by this charging profile have been flushed out, use one of the following commands, as applicable:

- For the GGSN or P-GW—**show unified-edge ggsn-pgw charging transfer status transport-profile-name *profile-name***
- For the S-GW—**show unified-edge sgw charging transfer status transport-profile-name *profile-name***
- To explicitly end any subscriber sessions, use one of the following commands, as applicable:
 - For the GGSN or P-GW—**clear unified-edge ggsn-pgw subscribers charging charging-profile *profile-name* gateway *gateway-name***
 - For the S-GW—**clear unified-edge sgw subscribers charging charging-profile *profile-name* gateway *gateway-name***
- To explicitly flush all the CDRs for the transport profile referred to by this charging profile, use the one of the following commands, as applicable:
 - For the GGSN or P-GW—**clear unified-edge ggsn-pgw charging cdr transport-profile-name *profile-name* gateway-name *name***
 - For the S-GW—**clear unified-edge sgw charging cdr transport-profile-name *profile-name* gateway-name *name***

Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.

Related Documentation	<ul style="list-style-type: none">• charging-profiles on page 780• Changing a Charging Profile on page 402• Mobility Maintenance Mode Overview on page 394
------------------------------	--

service-mode (Transport Profiles)

Syntax	<code>service-mode maintenance;</code>
Hierarchy Level	<code>[edit unified-edge gateways ggsn-pgw gateway-name charging transport-profiles profile-name],</code> <code>[edit unified-edge gateways sgw gateway-name charging transport-profiles profile-name]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the <code>[edit unified-edge gateways sgw gateway-name charging transport-profiles profile-name]</code> hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Place the respective transport profile under maintenance mode.</p> <p>To make the following changes to the existing transport profile configuration, you must put that transport profile in maintenance mode:</p> <ul style="list-style-type: none">• Change the CDR encoding format to comply with a different 3GPP technical specification release (that is, changing the <code>cdr-release</code> configuration)• Delete the transport profile <p>In maintenance mode, no new subscribers are accepted for that transport profile. However, the maintenance mode does not become active until no existing subscriber sessions are using that transport profile and all corresponding CDRs have been flushed out. Unless the maintenance mode becomes active, you cannot modify the above-mentioned transport profile attributes or delete the transport profile. Use the following commands to help you with the maintenance mode tasks:</p> <ul style="list-style-type: none">• To verify that the transport profile has entered active maintenance mode, use one of the following commands, as applicable:<ul style="list-style-type: none">• For the gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW)—<code>show unified-edge ggsn-pgw charging service-mode gateway gateway-name transport-profile profile-name</code>• For the Serving Gateway (S-GW)—<code>show unified-edge sgw charging service-mode gateway gateway-name transport-profile profile-name</code>• To verify that the subscriber count has reached zero, use one of the following commands, as applicable:<ul style="list-style-type: none">• For the GGSN or P-GW—<code>show unified-edge ggsn-pgw subscribers charging transport-profile profile-name gateway gateway-name</code>• For the S-GW—<code>show unified-edge sgw subscribers charging transport-profile profile-name gateway gateway-name</code>• To verify that all CDRs for the transport profile have been flushed out, use one of the following commands, as applicable:<ul style="list-style-type: none">• For the GGSN or P-GW—<code>show unified-edge ggsn-pgw charging transfer status transport-profile-name profile-name</code>

- For the S-GW—**show unified-edge sgw charging transfer status transport-profile-name *profile-name***
- To explicitly end any subscriber sessions, use one of the following commands, as applicable:
 - For the GGSN or P-GW—**clear unified-edge ggsn-pgw subscribers charging transport-profile *profile-name* gateway *gateway-name***
 - For the S-GW—**clear unified-edge sgw subscribers charging transport-profile *profile-name* gateway *gateway-name***
- To explicitly flush all the CDRs for the transport profile, use one of the following commands, as applicable:
 - For the GGSN or P-GW—**clear unified-edge ggsn-pgw charging cdr transport-profile-name *profile-name***
 - For the S-GW—**clear unified-edge sgw charging cdr transport-profile-name *profile-name***

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [transport-profiles on page 843](#)
- [Changing a Transport Profile on page 403](#)
- [Mobility Maintenance Mode Overview on page 394](#)

sgsn-mme-change-limit (Serving Gateway)

Syntax	sgsn-mme-change-limit <i>value</i> ;
Hierarchy Level	[edit unified-edge gateways sgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i> offline]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Configure the maximum number of serving GPRS support node (SGSN) or Mobility Management Entity (MME) changes that can occur before the Charging Data Record (CDR) is updated and closed.
Options	<p>value—Maximum number of SGSN or MME changes.</p> <p>Range: 1 through 5.</p> <p>Default: 4</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • offline on page 816 • Configuring Charging Trigger Events on page 296 • Configuring Charging on page 279

sgsn-sgw-change-limit (GGSN or P-GW)

Syntax	<code>sgsn-sgw-change-limit <i>value</i>;</code>
Hierarchy Level	[edit unified-edge gateways <i>ggsn-pgw gateway-name</i> charging trigger-profiles <i>profile-name</i> offline]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the maximum number of Serving GPRS Support Node (SGSN) or Serving Gateway (S-GW) changes that can occur before the CDR is updated and closed.
Options	<i>value</i> —Maximum number of SGSN or S-GW changes. Range: 1 through 5. Default: 4
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• offline on page 816• Configuring Charging Trigger Events on page 296• Configuring Charging on page 279

source-interface (GTP Prime)

Syntax	<pre>source-interface { interface-name; ipv4-address address; }</pre>
Hierarchy Level	<pre>[edit unified-edge gateways ggsn-pgw gateway-name charging gtp], [edit unified-edge gateways ggsn-pgw gateway-name charging gtp peer peer-name], [edit unified-edge gateways sgw gateway-name charging gtp], [edit unified-edge gateways sgw gateway-name charging gtp peer peer-name]</pre>
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W.</p> <p>Support at the <code>[edit unified-edge gateways sgw gateway-name charging gtp]</code> and <code>[edit unified-edge gateways sgw gateway-name charging gtp peer peer-name]</code> hierarchy levels introduced in Junos OS Mobility Release 11.4W.</p>
Description	<p>Configure the name of the local loopback interface and its IPv4 address as the source interface from which the GTP Prime packets are sent to the charging gateway function (CGF) servers. This is a mandatory configuration. However, before specifying this configuration, make sure that the interface has been previously defined.</p> <p>The following is a sample configuration:</p> <pre>gtp { source-interface { lo0.0; ipv4-address 10.10.10.10; } }</pre> <p>When there are global-level and peer-level configurations, the peer-level configuration takes precedence.</p>
Options	<p>address—IPv4 address of the local loopback interface from which the GTP Prime packets are sent. This is a mandatory configuration.</p> <p>interface-name—Name of the local loopback interface from which the GTP Prime packets are sent. This is a mandatory configuration.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • gtp on page 807 • peer (GTP Prime) on page 817 • Configuring GTP Prime for Charging on page 289 • Configuring GTP Prime Peers on page 290 • Configuring Charging on page 279

switch-back-time

Syntax	<code>switch-back-time seconds;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways], [edit unified-edge gateways sgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	The charging data function (CDF) transmits Charging Data Records (CDRs) to the highest-priority peer. The priority is determined by the peer-order configuration. If for any reason the highest-priority peer goes down, the CDF transmits the CDRs to the next high-priority peer and so on. If none of the peers are up, then the CDRs are transmitted to the local Routing Engine disk, if it is configured. During this transmission, it is possible that a peer or a peer that is higher in priority might come up. Instead of immediately switching over the transmission of the CDRs to the peer that recently came up, you can configure the duration that the CDF must wait to transmit the CDRs to the highest-priority peer that becomes available after this duration.



NOTE: If all the peers are down, in order not to lose any CDR data, you might want to configure the local storage on the Routing Engine disk using the following statement:

- `set unified-edge gateways ggsn-pgw gateway-name charging transport-profiles profile-name offline charging-gateways persistent-storage-order local-storage` for the gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW).
- `set unified-edge gateways sgw gateway-name charging transport-profiles profile-name offline charging-gateways persistent-storage-order local-storage` for the Serving Gateway (S-GW).

However, even if the Routing Engine disk is not configured for storage, the CDR data is not lost because it gets buffered in the services PICs. Services PICs can buffer up to a maximum of 2 GB of data, after which a call admission control (CAC) is triggered.

In the meantime, if one or multiple peers come alive, then CDF waits for the configured `switch-back-time` duration and routes the CDRs to the highest-priority peer that is alive after this duration. The CDRs that were stored previously on the Routing Engine disk are not routed to the charging gateway (peer) and remain on the disk. You need to transfer the CDRs using SSH FTP (SFTP) from the following location on the disk:
`/opt/mobility/charging/ggsn/final_log.`

Options	<p>seconds—Time, in seconds, CDF waits before transmitting the CDRs to the highest-priority peer.</p> <p>Range: 0 through 300 seconds</p> <p>Default: 30 seconds</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • charging-gateways on page 779 • Configuring Transport Profiles on page 295 • Configuring Charging on page 279

t3-response (GTP Prime)

Syntax	<code>t3-response response-interval;</code>
Hierarchy Level	<p>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging gtp],</p> <p>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>],</p> <p>[edit unified-edge gateways sgw <i>gateway-name</i> charging gtp],</p> <p>[edit unified-edge gateways sgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>]</p>
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W.</p> <p>Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging gtp] and [edit unified-edge gateways sgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>] hierarchy levels introduced in Junos OS Mobility Release 11.4W.</p>
Description	<p>Configure the duration (in seconds) that the charging data function (CDF) must wait before resending a GTP Prime message when the response to a request has not been received.</p> <p>When there are global-level and peer-level configurations, the peer-level configuration takes precedence.</p>
Options	<p>response-interval—Time that the CDF waits before resending a GTP Prime message when the response to a request has not been received.</p> <p>Range: 1 through 5 seconds</p> <p>Default: 5 seconds</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • gtp on page 807 • peer (GTP Prime) on page 817 • Configuring GTP Prime for Charging on page 289 • Configuring GTP Prime Peers on page 290 • Configuring Charging on page 279


tariff-time-list

Syntax	<pre>tariff-time-list { [tariff-time]; }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i>], [edit unified-edge gateways sgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i>] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure a list of local times (in hh:mm format) at which the tariff changes and Charging Data Records (CDRs) are generated to reflect the change in tariff. Because you can configure multiple values, make sure that there is a difference of at least 15 minutes between these values. You can configure up to a maximum of 24 values.</p> <p>Any change to the existing configuration applies to both existing and new subscriber sessions.</p>
Options	tariff-time —Local time at which to generate a CDR, in hh:mm format, when the tariff changes.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• trigger-profiles on page 846• Configuring Charging Trigger Events on page 296• Configuring Charging on page 279

time-limit

Syntax	<code>time-limit <i>value</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i> offline], [edit unified-edge gateways sgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i> offline]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i> offline] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the duration, in seconds, (since the previous trigger) after which the Charging Data Record (CDR) is updated with the uplink and downlink bytes transmitted in this duration and is closed. For example, if the duration is set to 3600 seconds, then the total resource utilization for the past hour is added to the CDR and the CDR is closed.</p> <p>Any change to the existing configuration does not affect a previously established session. The updated configuration applies only to new sessions.</p>
Options	<p>value—Duration in seconds.</p> <p>Range: 600 through 65,535 seconds</p> <p>Default: 0, indicates that no time limit is set.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • offline on page 816 • Configuring Charging Trigger Events on page 296 • Configuring Charging on page 279

traceoptions (Charging)

Syntax	<pre> traceoptions { file <i>file-name</i> <files <i>number</i>> <no-world-readable world-readable> <size <i>size</i>>; flag <i>flag</i>; level (all critical error info notice verbose warning); no-remote-trace; } </pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify tracing options for charging.
Options	<p>file <i>file-name</i>—Name of the file to receive the output of the tracing operation. The router appends -msfpc#pic# to the filename and places the file in the /var/log directory. For example, if you configured the filename as smd, then the actual log filename on the router is smd-ms50, where ms stands for multiservices card, and 5 and 0 are the FPC and PIC slot numbers.</p> <p>Range: 1 through 1024 bytes</p> <p>files <i>number</i>—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>Range: 2 through 1000 files</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Specify which operations are to be traced. To specify more than one operation, include multiple flag statements.</p>
	<div>  <p>CAUTION: You might want to enable traceoptions only when you want to debug specific charging operations. Enabling the traceoption flags might have an impact on the system performance.</p> </div>
	<ul style="list-style-type: none"> • all—Trace all operations of all charging submodules. • cdr-encoding—Trace ASN1 encoding of the CDRs. • client-fsm—Trace the charging-specific finite state machine (FSM) in the application framework (mobile-smd). • config—Trace configuration events on both daemons (chargemand and mobile-smd). • fsm—Trace FSM. • general—Trace general events that do not fit in any specific traces, such as errors in chargemand.

- **group-fsm**—Trace the transport-profile FSM in chargemand.
- **init**—Trace initialization events.
- **ipc**—Trace the interprocess communication (IPC) messages between mobile-smd and chargemand.
- **path-management**—Trace path management operations within the path manager module within chargemand.
- **request**—This flag is currently disabled.
- **resource**—Trace resources, such as memory, counters, and so on.
- **response**—This flag is currently disabled.
- **timers**—Trace resources associated with timer processing.
- **transport**—Trace transport-profile-level operations in chargemand.
- **triggers**—Trace trigger-profile-related operations used by the mobile-smd charging module.

level—Level of tracing to perform. You can specify any of the following levels:

- **all**—Match all levels.
- **critical**—Match error conditions.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match conditions that must be handled specially.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

no-remote-trace—(Optional) Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size size—(Optional) Maximum size of each trace file, in kilobytes (KB) or megabytes (MB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When the trace-file again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then, the oldest trace file is overwritten. If you specify a maximum number of files, you must also specify a maximum file size with the size option.

Syntax: *xk* to specify KB, *xm* to specify MB, or *xg* to specify GB.

Range: 10,240 through 1,073,741,824 bytes

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• charging on page 775• Tracing Charging Operations on page 302

traceoptions (Local Persistent Storage)

Syntax	<pre> traceoptions { file <i>file-name</i> <files <i>number</i>> <match <i>regular-expression</i>> <no-world-readable world-readable> <size <i>size</i>>; flag <i>flag</i>; level (all critical error info notice verbose warning); no-remote-trace; } </pre>
Hierarchy Level	<p>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging local-persistent-storage-options],</p> <p>[edit unified-edge gateways sgw <i>gateway-name</i> charging local-persistent-storage-options]</p>
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W.</p> <p>Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging local-persistent-storage-options] hierarchy level introduced in Junos OS Mobility Release 11.4W.</p>
Description	Specify tracing options related to the storage of Charging Data Records (CDRs) on the local Routing Engine disk.
Options	<p>file <i>filename</i>—Name of the file to receive the output of the tracing operation.</p> <p>Range: 1 through 1024 bytes</p> <p>files <i>number</i>—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>Range: 2 through 1000 files</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Specify which operations are to be traced. To specify more than one operation, include multiple flag statements.</p>



CAUTION: You may want to enable traceoptions only when you want to debug specific charging operations. Enabling the traceoption flags might have an impact on the system performance.

- **all**—Trace all operations.
- **connection**—Trace the connection establishment between Routing Engine and all services PICs for CDR file backup.
- **file-operations**—Trace all file open, write, and close operations.
- **general**—Trace general operations.

- **journaling**—Trace journaling operations. Journaling creates a log for each file-write operation, which helps to sanitize the CDR data in temporary log files after a reboot.
- **mirror**—Trace mirroring operations. Mirroring enables you to synchronize the CDR file information onto backup.

level—Level of tracing to perform. You can specify any of the following levels:

- **all**—Match all levels.
- **critical**—Match critical conditions.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match conditions that must be handled specially.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

match *regex*—(Optional) Refine the output to include lines that contain the regular expression (*regex*).

no-remote-trace—(Optional) Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB) or megabytes (MB). When a trace file named *trace-file* reaches this size, it is renamed **trace-file.0**. When the trace-file again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and *trace-file* is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then, the oldest trace file is overwritten. If you specify a maximum number of files, you must also specify a maximum file size with the *size* option.

Syntax: *xk* to specify KB, *xm* to specify MB, or *xg* to specify GB.

Range: 10,240 through 1,073,741,824 bytes


Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level	interface—To view this statement in the configuration.
	interface-control—To add this statement to the configuration.

Related Documentation	• local-persistent-storage-options on page 810
	• Configuring Persistent Storage on page 291

transport-profile

Syntax	<code>transport-profile <i>profile-name</i>;</code>
Hierarchy Level	<code>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i>],</code> <code>[edit unified-edge gateways sgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i>]</code>
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W.</p> <p>Support at the <code>[edit unified-edge gateways sgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i>]</code> hierarchy level introduced in Junos OS Mobility Release 11.4W.</p>
Description	<p>Associate a transport profile with a charging profile. However, make sure this profile has been previously defined. This is a mandatory configuration.</p> <p>When a subscriber session is created, the subscriber is bound to a charging profile and the transport profile configuration associated with this profile determines the transport of the CDRs generated for this subscriber from the charging data function (CDF) to the external charging gateway function (CGF) servers or the local Routing Engine disk, or both.</p> <p>Any modification to the existing configuration of this attribute must be done only when the charging profile with which it is associated is under active maintenance mode. Use one of the following commands, as applicable, to bring the charging profile under maintenance mode:</p> <ul style="list-style-type: none"> For the gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW)—<code>set unified-edge gateways ggsn-pgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i> service-mode maintenance</code> For the Serving Gateway (S-GW)—<code>set unified-edge gateways sgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i> service-mode maintenance</code> <div style="margin-top: 20px;">  <p>TIP: If the profile is not already defined, use one of the following commands, as applicable, to define a new transport profile:</p> <ul style="list-style-type: none"> GGSN or P-GW—<code>set unified-edge gateways ggsn-pgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i></code> S-GW—<code>set unified-edge gateways sgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i></code> </div>
Options	<i>profile-name</i> —Name of the transport profile to be associated with the charging profile.
Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.

- Related Documentation**
- [charging-profiles on page 780](#)
 - [Configuring Charging Profiles on page 300](#)
 - [Charging Profiles on page 277](#)
 - [Configuring Charging on page 279](#)


transport-profiles

Syntax	<pre> transport-profiles <i>profile-name</i> { description <i>string</i>; offline { charging-gateways { cdr-aggregation-limit <i>value</i>; cdr-release (r7 r8 r99); mtu <i>value</i>; peer-order { [peer <i>charging-gateway-peer-name</i>]; } persistent-storage-order { local-storage; } switch-back-time <i>seconds</i>; } } service-mode maintenance; } </pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging], [edit unified-edge gateways sgw <i>gateway-name</i> charging]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure a transport profile, which determines how the Charging Data Records (CDRs) are transported from the charging data function (CDF) to a storage resource, which can be external charging gateway function (CGF) servers or the local Routing Engine disk, or both. This is a mandatory configuration.</p> <p>You can configure up to a maximum of eight transport profiles.</p> <p>The remaining statements are explained separately.</p>
Options	<p><i>profile-name</i>—Name of the transport profile.</p> <p>Range: 1 through 128 bytes</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • charging on page 775 • Configuring Transport Profiles on page 295 • Configuring Charging on page 279

transport-protocol (GTP Prime)

Syntax	<code>transport-protocol (tcp udp);</code>
Hierarchy Level	<code>[edit unified-edge gateways ggsn-pgw gateway-name charging gtp],</code> <code>[edit unified-edge gateways ggsn-pgw gateway-name charging gtp peer peer-name],</code> <code>[edit unified-edge gateways sgw gateway-name charging gtp],</code> <code>[edit unified-edge gateways sgw gateway-name charging gtp peer peer-name]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the <code>[edit unified-edge gateways sgw gateway-name charging gtp]</code> and <code>[edit unified-edge gateways sgw gateway-name charging gtp peer peer-name]</code> hierarchy levels introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the transport protocol for transmitting the GTP Prime packets from the charging data function (CDF) to the charging gateway function (CGF) server, which can be either GTP Prime over UDP or GTP Prime over TCP.</p> <p>When there are global-level and peer-level configurations, the peer-level configuration takes precedence.</p>
Options	<p><code>tcp</code>—Transport protocol used is TCP.</p> <p><code>udp</code>—Transport protocol used is UDP.</p>
Required Privilege Level	<p><code>interface</code>—To view this statement in the configuration.</p> <p><code>interface-control</code>—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• gtp on page 807• peer (GTP Prime) on page 817• Configuring GTP Prime for Charging on page 289• Configuring GTP Prime Peers on page 290• Configuring Charging on page 279

trigger-profile

Syntax	<code>trigger-profile <i>profile-name</i>;</code>
Hierarchy Level	<code>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i>],</code> <code>[edit unified-edge gateways sgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i>]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the <code>[edit unified-edge gateways sgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i>]</code> hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Associate a trigger profile with a charging profile. However, make sure this profile has been previously defined. When a subscriber session is created, the subscriber is bound to a charging profile and the trigger profile configuration associated with this profile determines the events that result in the creation of a CDR, the addition of a container to a CDR, and the closure of a CDR.
<div>  <div> <p>TIP: If the profile is not already defined, use one of the following commands, as applicable, to define a new trigger profile:</p> <ul style="list-style-type: none"> For the gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW)—<code>set unified-edge gateways ggsn-pgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i></code> For the Serving Gateway (S-GW)—<code>set unified-edge gateways sgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i></code> </div> </div>	
Options	<i>profile-name</i> —Name of the trigger profile to be associated with the charging profile.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> charging-profiles on page 780 Configuring Charging Profiles on page 300 Charging Profiles on page 277 Configuring Charging on page 279

trigger-profiles

Syntax `trigger-profiles profile-name {
 description string;
 offline {
 container-limit value;
 exclude {
 ms-timezone-change;
 plmn-change;
 qos-change;
 rat-change;
 sgsn-mme-change; #S-GW only
 sgsn-sgw-change; #P-GW only
 user-location-change;
 }
 sgsn-mme-change-limit value; #S-GW only
 sgsn-sgw-change-limit value; #P-GW only
 time-limit value;
 volume-limit {
 value;
 direction (both | uplink);
 }
 }
 tariff-time-list {
 tariff-time;
 }
}`

Hierarchy Level [edit unified-edge gateways *ggsn-pgw gateway-name* charging],
 [edit unified-edge gateways *sgw gateway-name* charging]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.
 Support at the [edit unified-edge gateways *sgw gateway-name* charging] hierarchy level introduced in Junos OS Mobility Release 11.4W.

Description Configure a trigger profile, which determines the events that trigger the creation of a Charging Data Record (CDR), 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 CDR profile determines the content of a CDR, whereas the transport profile determines how the generated CDRs are transmitted to the charging gateway function (CGF) server.

The remaining statements are explained separately.

Options *profile-name*—Name of the trigger profile.

Values: 1 through 128 bytes

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [charging on page 775](#)
- [Configuring Charging Trigger Events on page 296](#)
- [Configuring Charging on page 279](#)

user-name (Local Persistent Storage)

Syntax `user-name string;`

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name* charging local-persistent-storage-options],
[edit unified-edge gateways sgw *gateway-name* charging local-persistent-storage-options]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.
Support at the [edit unified-edge gateways sgw *gateway-name* charging local-persistent-storage-options] hierarchy level introduced in Junos OS Mobility Release 11.4W.

Description Restrict access to the Charging Data Record (CDR) files to a specific user.

In addition to the non-root user who is authorized using this statement, the root user always has access permissions.

Options *string*—Username.
Values: 1 through 32 bytes

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [local-persistent-storage-options on page 810](#)
- [Configuring Persistent Storage on page 291](#)
- [Configuring Charging on page 279](#)

version (GTP Prime)

Syntax	<code>version (v0 v1 v2);</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging gtp], [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>], [edit unified-edge gateways sgw <i>gateway-name</i> charging gtp], [edit unified-edge gateways sgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging gtp] and [edit unified-edge gateways sgw <i>gateway-name</i> charging gtp peer <i>peer-name</i>] hierarchy levels introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the latest GTP Prime version that is supported on the configured local loopback source interface's IP address from which the GTP Prime packets are sent to the charging gateway function (CGF) server. The possible values are: v0, v1, or v2.</p> <p>When there are global-level and peer-level configurations, the peer-level configuration takes precedence.</p>
Options	<p>v0—GTP Prime version supported is v0.</p> <p>v1—GTP Prime version supported is v1.</p> <p>v2—GTP Prime version supported is v2.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• gtp on page 807• peer (GTP Prime) on page 817• Configuring GTP Prime for Charging on page 289• Configuring GTP Prime Peers on page 290• Configuring Charging on page 279

visitor-profile

Syntax	<code>visitor-profile <i>visitor-profile</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> apn-services apns <i>name</i> charging], [edit unified-edge gateways sgw <i>gateway-name</i> charging global-profile]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging global-profile] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Specify the profile that should be used to charge visiting subscribers. If the profile-selection-order configuration indicates static , then this profile is used for visiting subscribers.



NOTE: The charging profile must already be configured on the broadband gateway.

The broadband gateway determines whether the subscriber is a visitor by using 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). If the subscriber's International Mobile Subscriber Identity (IMSI), MCC, and MNC do not belong to the PLMN to which both the GGSN or P-GW and the S-GW belong, then the subscriber is deemed a visitor and the **visitor-profile** is applied. If the **visitor-profile** is not configured, then the **default-profile**, if configured, is applied. If the **default-profile** is also not configured, then the subscriber session is created with no charging applied.

Options	<i>visitor-profile</i> —Name of the visitor profile.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 119 • Configuring S-GW Global Charging Profiles and Selection Order on page 282 • charging (APN) on page 695 • charging-profiles on page 780 • global-profile (Serving Gateway) on page 806

volume-limit

Syntax	<pre>volume-limit { value; direction (both uplink); }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i> offline], [edit unified-edge gateways sgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i> offline]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i> offline] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the volume of data, in bytes, that is transmitted (since the previous trigger) before the Charging Data Record (CDR) is updated with the transmitted bytes and is closed. In addition, you can specify whether the maximum volume of data transmitted includes the data transmitted in both the uplink and downlink directions, or only in the uplink direction.</p> <p>Any change to the existing configuration does not affect a previously established session. The updated configuration applies only to new sessions.</p>
Default	If you do not include the volume-limit statement, the volume limit trigger is disabled.
Options	<p>value—Maximum volume of data transmitted, in bytes, after which the CDR is updated and closed.</p> <p>Range: 1 through 4 GB</p> <p>The remaining statement is explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• offline on page 816• Configuring Charging Trigger Events on page 296• Configuring Charging on page 279

watermark-level-1

Syntax	<pre>watermark-level-1 { notification-level (both snmp-alarm syslog); percentage <i>value</i>; }</pre>
Hierarchy Level	<p>[edit unified-edge gateways <i>ggsn-pgw gateway-name</i> charging local-persistent-storage-options disk-space-policy], [edit unified-edge gateways <i>sgw gateway-name</i> charging local-persistent-storage-options disk-space-policy]</p>
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways <i>sgw gateway-name</i> charging local-persistent-storage-options disk-space-policy] hierarchy level introduced in Junos OS Mobility Release 11.4W.</p>
Description	<p>Configure the percentage of Routing Engine disk space to be used for storage and the action to be taken when this limit is reached, such as raise SNMP alarms, record the alert information in the system logs, or both. You can then take appropriate measures to prevent any loss of Charging Data Record (CDR) data.</p>
Options	<p>notification-level (both snmp-alarm syslog)—Specify whether you want to raise SNMP alarms, log information on the system logs, or both, when the watermark level is reached.</p> <ul style="list-style-type: none"> • both—Log the alert information on system log files and also raise an SNMP alarm. • snmp-alarm—Raise an SNMP alarm. • syslog—Log the alert information on system log files. <p>Default: syslog</p> <p>percentage <i>value</i>—Percentage of Routing Engine disk space to be used for storage after which you get an alert (if it is configured). Entering 0 disables the checking for the watermark level.</p> <p>Default: 70 percent of the Routing Engine disk space</p>
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • disk-space-policy on page 790 • Configuring Persistent Storage on page 291 • Configuring Charging on page 279

watermark-level-2

Syntax	<pre>watermark-level-2 { notification-level (both snmp-alarm syslog); percentage <i>value</i>; }</pre>
Hierarchy Level	[edit unified-edge gateways <i>ggsn-pgw gateway-name</i> charging local-persistent-storage-options disk-space-policy], [edit unified-edge gateways <i>sgw gateway-name</i> charging local-persistent-storage-options disk-space-policy]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways <i>sgw gateway-name</i> charging local-persistent-storage-options disk-space-policy] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Configure the percentage of Routing Engine disk space to be used for storage and also the action to be taken when this limit is reached, such as raise SNMP alarms, record the alert information in the system logs, or both. You can then take appropriate measures to prevent any loss of Charging Data Record (CDR) data.
Options	<p>notification-level (both snmp-alarm syslog)—Specify whether you want to raise SNMP alarms, log information on the system logs, or both when the watermark level is reached.</p> <ul style="list-style-type: none">• both—Log the alert information on system log files and raise an SNMP alarm.• snmp-alarm—Raise an SNMP alarm.• syslog—Log the alert information on system log files. <p>Default: syslog</p> <p>percentage <i>value</i>—Percentage of Routing Engine disk space to be used for storage after which you get an alert (if it is configured). Entering 0 disables the checking for the watermark level.</p> <p>Default: 80 percent of the Routing Engine disk space</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• disk-space-policy on page 790• Configuring Persistent Storage on page 291• Configuring Charging on page 279

watermark-level-3

Syntax	<pre>watermark-level-3 { notification-level (both snmp-alarm syslog); percentage <i>value</i>; }</pre>
Hierarchy Level	<p>[edit unified-edge gateways <i>ggsn-pgw gateway-name</i> charging local-persistent-storage-options disk-space-policy], [edit unified-edge gateways <i>sgw gateway-name</i> charging local-persistent-storage-options disk-space-policy]</p>
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways <i>sgw gateway-name</i> charging local-persistent-storage-options disk-space-policy] hierarchy level introduced in Junos OS Mobility Release 11.4W.</p>
Description	<p>Configure the percentage of Routing Engine disk space to be used for storage and also the action to be taken when this limit is reached, such as raise SNMP alarms, record the alert information in the system logs, or both.</p> <p>When this watermark level is reached, the charging daemon stops writing the Charging Data Records (CDRs) to the local Routing Engine disk till the CDR storage space is restored by transferring the files using SSH FTP (SFTP) and deleting the files from the CDR log directory. However, the data is not immediately lost because the services PICs buffer up to 2 GB of data.</p>
Options	<p>notification-level (both snmp-alarm syslog)—Specify whether you want to raise SNMP alarms, log information on the system logs, or both when the watermark level is reached.</p> <ul style="list-style-type: none"> both—Log the alert information on system log files and also raise an SNMP alarm. snmp-alarm—Raise an SNMP alarm. syslog—Log the alert information on system log files. <p>Default: syslog</p> <p>percentage <i>value</i>—Percentage of Routing Engine disk space to be used for storage after which you get an alert (if it is configured). Entering 0 disables the checking for the watermark level.</p> <p>Default: 90 percent of the Routing Engine disk space</p>
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> disk-space-policy on page 790 Configuring Persistent Storage on page 291 Configuring Charging on page 279

world-readable (Local Persistent Storage)

Syntax	world-readable;
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging local-persistent-storage-options], [edit unified-edge gateways sgw <i>gateway-name</i> charging local-persistent-storage-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> charging local-persistent-storage-options] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Allow all users to have read permissions on the Charging Data Record (CDR) files. By default, this is disabled.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• local-persistent-storage-options on page 810• Configuring Persistent Storage on page 291• Configuring Charging on page 279

Class of Service (CoS) Configuration Statements

aggregated-maximum-bit-rate

Syntax	<pre>aggregated-maximum-bit-rate { downlink x; reject; upgrade; uplink y; }</pre>
Hierarchy Level	[edit unified-edge cos-cac cos-policy-profiles <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the aggregated maximum bit rate (AMBR) for all default bearers associated with a specific gateway or access point name. The AMBR specifies the total maximum bit rate and is configured separately for uplink and downlink traffic. 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.
Options	<p>downlink—Aggregated maximum bit rate for downlink traffic.</p> <p>reject—Aggregated maximum bit rate to be rejected.</p> <p>uplink—Aggregated maximum bit rate for uplink traffic.</p> <p>upgrade—Aggregated maximum bit rate value to be upgraded.</p> <p>Range: 1 through 1,000,000 Kbps</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring QoS on the Broadband Gateway Overview on page 323 • cos-policy-profiles on page 868


allocation-retention-priority

Syntax	<pre>allocation-retention-priority { gtpv1-priority-value <i>priority-value</i> [upgrade] ; gtpv2-priority-value <i>priority-value</i> [upgrade] ; }</pre>
Hierarchy Level	[edit unified-edge cos-cac cos-policy-profiles <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the allocation and retention priority (ARP) value to the local policy. The bearer requests with a higher ARP than the configured ARP value are accepted when thresholds are exceeded at the APN level or system level. The ARP value of a low priority bearer request is allowed for an upgrade.
Options	<p><i>gtpv1</i>—Priority value for ARP policy configuration. Range: <i>gtpv1</i>—1 through 3.</p> <p><i>gtpv2</i>—Priority value for ARP policy configuration Range: <i>gtpv2</i>—1 through 15</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring QoS on the Broadband Gateway Overview on page 323• cos-policy-profiles on page 868

anchor-pfe-default-bearers-percentage (Serving Gateway)

Syntax	anchor-pfe-default-bearers-percentage <i>default-bearers-percentage</i> ;
Hierarchy Level	[edit unified-edge gateways sgw <i>gateway-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Configure the maximum number of Evolved Packet System (EPS) default bearers allowed for each anchor Packet Forwarding Engine on the Serving Gateway (S-GW). This value is specified as a percentage of the maximum number of EPS default bearers allowed for an anchor Packet Forwarding Engine.
Options	<p>default-bearers-percentage—Maximum number of EPS default bearers per anchor Packet Forwarding Engine, specified as a percentage of the maximum number of EPS default bearers or allowed.</p> <p>Range: 10 through 100 percent</p> <p>Default: 100 percent, which indicates that there is no restriction on the maximum number of EPS default bearers admitted on an anchor Packet Forwarding Engine. The only limitation is that the total number of bearers admitted on the anchor Packet Forwarding Engine cannot exceed the maximum number of bearers allowed for an anchor Packet Forwarding Engine.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • anchor-pfe-guaranteed-bandwidth (Serving Gateway) on page 858 • anchor-pfe-maximum-bearers (Serving Gateway) on page 859 • Configuring S-GW-Specific CAC Parameters on page 384

anchor-pfe-guaranteed-bandwidth (Serving Gateway)

Syntax	<code>anchor-pfe-guaranteed-bandwidth <i>anchor-pfe-guaranteed-bandwidth</i>;</code>
Hierarchy Level	[edit unified-edge gateways sgw <i>gateway-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Configure the guaranteed bandwidth for each anchor Packet Forwarding Engine on the Serving Gateway (S-GW). This value limits the bandwidth available to guaranteed bit rate (GBR) bearers on an anchor Packet Forwarding Engine, which in turn limits the number of GBR bearers that can be created on an anchor Packet Forwarding Engine.
	<div><p>NOTE: Configuring a value that is more than the actual physical bandwidth of the anchor Packet Forwarding Engine results in oversubscription; in this scenario only a best-effort service can be provided.</p></div>
Options	<p><i>anchor-pfe-guaranteed-bandwidth</i>—Guaranteed bandwidth per anchor Packet Forwarding Engine.</p> <p>Range: 10 through 100 gigabits per second (Gbps)</p> <p>Default: 40 Gbps</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• anchor-pfe-default-bearers-percentage (Serving Gateway) on page 857• anchor-pfe-maximum-bearers (Serving Gateway) on page 859• Configuring S-GW-Specific CAC Parameters on page 384

anchor-pfe-maximum-bearers (Serving Gateway)

Syntax	anchor-pfe-maximum-bearers <i>maximum-bearers</i> ;
Hierarchy Level	[edit unified-edge gateways sgw <i>gateway-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Configure the maximum number of Evolved Packet System (EPS) bearers, both default and dedicated, allowed for each anchor Packet Forwarding Engine on the Serving Gateway (S-GW).
Options	<p><i>maximum-bearers</i>—Maximum number of EPS bearers, in multiples of one thousand, per anchor Packet Forwarding Engine.</p> <p>Range: 100 through 510,000 bearers</p> <p>Default: 510,000 bearers</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • anchor-pfe-default-bearers-percentage (Serving Gateway) on page 857 • anchor-pfe-guaranteed-bandwidth (Serving Gateway) on page 858 • Configuring S-GW-Specific CAC Parameters on page 384

bandwidth-pools

Syntax	<pre>bandwidth-pools { name { bandwidth x; traffic-class-bandwidth-pool conversational streaming percentage z <i>downgrade</i>; } }</pre>
Hierarchy Level	[edit unified-edge cos-cac]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the bandwidth pools for the class-of-service call admission control (CoS-CAC). Configuring a bandwidth pool provides sufficient bandwidth for bearers to be created or modified. The call admission control (CAC) uses the bandwidth pools to negotiate and reserve bandwidth.
Options	<p>name—Name of the bandwidth pool that can be attached to the access point name or the P-GW.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring QoS on the Broadband Gateway Overview on page 323• cos-cac on page 865

bearer-load

Syntax	<pre> bearer-load { low { gtpv1-arp y; gtpv2-priority-level z; percentage x; } high { gtpv1-arp y; gtpv2-priority-level z; percentage x; } } </pre>
Hierarchy Level	[edit unified-edge cos-cac resource-threshold-profiles]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the number of bearer load. The bearer load indicates a precise level of admission control when a bearer load reaches a configured lower or upper threshold. The bearer load is expressed as a percentage. If the bearer load is associated with the local policy, the gateway level low is 70 percent and the gateway high level is 85 percent.
Options	<p><i>high</i>—High threshold configuration. Range: <i>high</i>—70 percent</p> <p><i>low</i>—Low threshold configuration. Range: <i>low</i>—85 percent</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring QoS on the Broadband Gateway Overview on page 323 • resource-threshold-profiles on page 887

classifier-profile

Syntax	<code>classifier-profile <i>name</i>;</code>
Hierarchy Level	<code>[edit unified-edge local-policies <i>name</i>]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Define the mapping from the traffic class to the forwarding class (internal queues) and packet loss priority. You can configure separate classifier profiles for home, roaming, and visitor subscriber traffic.
Options	<i>name</i> —Classifier profile name.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring QoS on the Broadband Gateway Overview on page 323• local-policies on page 877

classifier-profiles

Syntax	<pre> classifier-profiles { name { traffic-class-classifier-profiles conversational streaming background forwarding-class fc-name1 loss-priority [low high]; traffic-class-classifier-profiles interactive traffic-handling-priority 1 2 3 forwarding-class fc-name1 loss-priority [low high]; qos-class-identifier x forwarding-class fc-name1 loss-priority [low high]; } } </pre>
Hierarchy Level	[edit unified-edge cos-cac]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Define the mapping from the traffic class to the forwarding class (internal queues) and the packet loss priority. A QoS classifier profile defines the QoS class identifiers for a P-GW. You configure QCI values to define the packet-forwarding treatment for each bearer. A QCI is associated with a priority, delay, and packet loss values. The broadband gateway supports only QCI values for services that do not require dedicated resource allocation for a guaranteed bit rate (GBR). A QoS classifier profile enables classifier tables for mobile subscribers on UMTS and EPS.</p>
Default	If you do not configure any CoS features, all packets are transmitted from the output transmission queue 0.
Options	<p>profile-name—Name of the classifier profile to be applied to this interface.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring QoS on the Broadband Gateway Overview on page 323 • cos-cac on page 865

class-of-service

Syntax	<pre>class-of-service { interfaces { mif. number { rewrite-rules { dscp rewrite-rule-name [protocol gtp-inet-both gtp-inet-outer]; dscp-ipv6 rewrite-rule-name [protocol gtp-inet-both gtp-inet-outer]; inet-precedence rewrite-rule-name [protocol gtp-inet-both gtp-inet-outer]; } ingress-rewrite-rules { dscp rewrite-rule-name; dscp-ipv6 rewrite-rule-name; inet-precedence rewrite-rule-name; } } } }</pre>
Hierarchy Level	[edit]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the class of service (CoS) for the 3GPP support for broadband gateways. At the first instance, you must configure the ingress and egress rewrite rules to set the value of the CoS bits within the IP header of upstream and downstream subscriber packets received on the mobile interface. Later, you must apply the ingress and egress rewrite rules to the mobile interface to set CoS values for upstream and downstream packets. Within ingress and egress, you can specify rewrite rules for DSCP v4, DSCP v6, or IP precedence values.
Options	The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring QoS on the Broadband Gateway Overview on page 323

cos-cac

```

Syntax classifier-profiles {
    name {
        traffic-class-classifier-profiles conversational | streaming | background
        forwarding-class fc-name1 loss-priority [low | high];
        traffic-class-classifier-profiles interactive traffic-handling-priority 1 | 2 | 3
        forwarding-class fc-name1 loss-priority [low | high];
        qos-class-identifier x forwarding-class fc-name1 loss-priority [low | high];
    }
}
bandwidth-pools {
    name {
        bandwidth x;
        traffic-class-bandwidth-pool conversational | streaming percentage z downgrade ;
    }
}
resource-threshold-profiles {
    name {
        system-load {
            low {
                gtpv1-arp y;
                gtpv2-priority-level z;
                percentage x;
            }
            high {
                gtpv1-arp y;
                gtpv2-priority-level z;
                percentage x;
            }
        }
        bearer-load {
            low {
                gtpv1-arp y;
                gtpv2-priority-level z;
                percentage x;
            }
            high {
                gtpv1-arp y;
                gtpv2-priority-level z;
                percentage x;
            }
        }
        cpu {
            low {
                gtpv1-arp y;
                gtpv2-priority-level z;
                percentage x;
            }
            high {
                gtpv1-arp y;
                gtpv2-priority-level z;
                percentage x;
            }
        }
        memory {
            low {

```

```

        gtpv1-arp y;
        gtpv2-priority-level z;
        percentage x;
    }
    high {
        gtpv1-arp y;
        gtpv2-priority-level z;
        percentage x;
    }
}
}
cos-policy-profiles {
    name {
        qci 5 to 9 [upgrade];
        traffic-class-cos-policy-profiles string priority z [upgrade];
        aggregated-maximum-bit-rate {
            downlink x;
            reject;
            upgrade;
            uplink y;
        }
        allocation-retention-priority {
            gtpv2-priority-value 1 to 15 [upgrade];
            gtpv1-priority-value 1 to 3 [upgrade];
        }
        maximum-bit-rate {
            traffic-class-cos-policy-profiles {
                any [both] | [uplink] | [downlink] x
                background [both] | [uplink] | [downlink] x
                conversational [both] | [uplink] | [downlink] x
                interactive [both] | [uplink] | [downlink] x
                reject;
                streaming [both] | [uplink] | [downlink] x
                upgrade;
            }
        }
        guaranteed-bit-rate {
            traffic-class-cos-policy-profiles {
                any [both] | [uplink] | [downlink] x
                conversational [both] | [uplink] | [downlink] x
                reject;
                streaming [both] | [uplink] | [downlink] x
                upgrade;
            }
        }
        exceed-action [drop | transmit];
        violate-action [set-loss-priority-high | transmit];
    }
}

```

Hierarchy Level [edit unified-edge]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description	Configure the set of parameters for the class-of-service call admission control. Call admission control on the broadband gateway ensures that the required network resources are available for real-time data traffic such as voice and video. Call admission control maintains information about all resources available on the broadband gateway and resources that have been allocated to bearers. A call admission is based on resource availability and the priority of the bearer, and allows the broadband gateway to reject or downgrade Create bearer or Modify bearer requests when the system, CPU, memory, or bearer load for upstream or downstream traffic exceeds the configured call admission control thresholds.
Default	If you do not configure any CoS features, all packets are transmitted from the output transmission queue 0.
Options	The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring QoS on the Broadband Gateway Overview on page 323

cos-policy-profile

Syntax	<code>cos-policy-profile <i>name</i> ;</code>
Hierarchy Level	<code>[edit unified-edge local-policies <i>name</i>]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Define policies for limiting, upgrading, or rejecting calls based on the requested QoS parameters. You can configure separate CoS profiles for home, roaming, and visitor subscriber traffic.
Options	<i>name</i> —CoS policy profile name.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring QoS on the Broadband Gateway Overview on page 323 • local-policies on page 877

cos-policy-profiles

```
Syntax  cos-policy-profiles {
        name {
            qci 5 to 9 [upgrade];
            traffic-class-cos-policy-profiles string priority z [upgrade] ;
            aggregated-maximum-bit-rate {
                downlink x ;
                reject ;
                upgrade ;
                uplink y ;
            }
            allocation-retention-priority {
                gtpv1-priority-value 1 to 3 [upgrade] ;
                gtpv2-priority-value 1 to 15 [upgrade] ;
            }
            maximum-bit-rate {
                traffic-class-cos-policy-profiles {
                    any [both] | [uplink] | [downlink] x
                    background [both] | [uplink] | [downlink] x
                    conversational [both] | [uplink] | [downlink] x
                    interactive [both] | [uplink] | [downlink] x
                    reject;
                    streaming [both] | [uplink] | [downlink] x
                    upgrade;
                }
            }
            guaranteed-bit-rate {
                traffic-class-cos-policy-profiles {
                    any [both] | [uplink] | [downlink] x
                    conversational [both] | [uplink] | [downlink] x
                    reject;
                    streaming [both] | [uplink] | [downlink] x
                    upgrade;
                }
            }
            exceed-action [drop | transmit];
            violate-action [set-loss-priority-high | transmit];
        }
    }
```

Hierarchy Level [edit unified-edge cos-cac]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Define the policies for limiting, upgrading, or rejecting calls based on the requested QoS parameters. For a 3G network, the CoS policy profile defines the highest traffic class that can be accepted at an APN or system level, the maximum bit rate and guaranteed bit rate for bearers, and the allocation and retention priority. For a 4G network, the CoS policy profile defines the highest QoS Class Identifier (QCI) value that can be accepted at the APN level or system level, the aggregated maximum bit rate (AMBR) for default bearers, and the allocation and retention priority.

Options *profile-name*—Name of the CoS policy profile.

The remaining statements are explained separately.

Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring QoS on the Broadband Gateway Overview on page 323

cpu

Syntax	<pre> cpu { low { gtpv1-arp y; gtpv2-priority-level z; percentage x; } high { gtpv1-arp y; gtpv2-priority-level z; percentage x; } } </pre>
Hierarchy Level	[edit unified-edge cos-cac resource-threshold-profiles <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the CPU load. The CPU load indicates a precise level of admission control when the CPU load reaches a configured lower or upper threshold.
Default	The bearer load is expressed as a percentage. If bearer load is associated with the local policy the gateway low level is 70 percent and the gateway high level is 85 percent.
Options	<p><i>high</i>—High threshold configuration.</p> <p><i>low</i>—Low threshold configuration.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring QoS on the Broadband Gateway Overview on page 323 • resource-threshold-profiles on page 887

dl-bandwidth-pool

Syntax	<code>dl-bandwidth-pool <i>name</i> ;</code>
Hierarchy Level	<code>[edit unified-edge local-policies <i>name</i>]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the limit for downlink bandwidth usage at the system or APN level.
Options	<i>name</i> —Name of the downlink bandwidth.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring QoS on the Broadband Gateway Overview on page 323• local-policies on page 877

dscp-ipv6

Syntax	<code>dscp-ipv6 <i>rewrite-rule-name</i> [protocol gtp-inet-both gtp-inet-outer];</code>
Hierarchy Level	<code>[edit class-of-service interfaces rewrite-rules]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Define the DiffServ Code Point (DSCP) rewrite rule and the protocol mapping for GTP <i>inet</i> for the packets for IPv6. This rule is applied to IPv6 packets going to the Packet Data Network (PDN) network.
Options	<i>rewrite-rule-name</i> —Name of the rewrite rule.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring QoS on the Broadband Gateway Overview on page 323• rewrite-rules on page 889

dscp-ipv6 (Ingress)

Syntax	<code>dscp-ipv6 rewrite-rule-name;</code>
Hierarchy Level	[edit class-of-service interfaces ingress-rewrite-rules]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Define the DiffServ code point (DSCP) rewrite rule and the mapping that is applied to the packets for IPv6. This rule is applied to IPv6 packets going to the core network.
Options	<i>rewrite-rule-name</i> —Name of the rewrite rule.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring QoS on the Broadband Gateway Overview on page 323 • ingress-rewrite-rules on page 875

dscp

Syntax	<code>dscp rewrite-rule-name [protocol gtp-inet-both gtp-inet-outer];</code>
Hierarchy Level	[edit class-of-service interfaces rewrite-rules]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Define the DiffServ Code Point (DSCP) rewrite rule and the protocol mapping for GTP inet that is applied to the packets. This rule is applied to packets going to the Packet Data Network (PDN).
Options	<i>rewrite-rule-name</i> —Name of the rewrite rule.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring QoS on the Broadband Gateway Overview on page 323 • rewrite-rules on page 889

dscp (Ingress)

Syntax	<code>dscp <i>rewrite-rule-name</i>;</code>
Hierarchy Level	[edit class-of-service interfaces ingress-rewrite-rules]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Define the DiffServ Code Point (DSCP) rewrite rule. This rule is applied to packets going to the core network.
Options	<i>rewrite-rule-name</i> —Name of the rewrite rule.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring QoS on the Broadband Gateway Overview on page 323• ingress-rewrite-rules on page 875

exceed-action

Syntax	<code>exceed-action [drop transmit]</code>
Hierarchy Level	[edit unified-edge cos-cac cos-policy-profiles <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Set the action to take when the specified levels for all CoS policy profile parameters are exceeded.
Options	<i>drop</i> —Set the drop levels for the CoS policy for exceed action. <i>transmit</i> —Set the transmit levels for exceed action.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring QoS on the Broadband Gateway Overview on page 323• cos-policy-profiles on page 868

guaranteed-bit-rate

Syntax	<pre> guaranteed-bit-rate { traffic-class-cos-policy-profiles { any [both] [uplink] [downlink] x conversational [both] [uplink] [downlink] x reject; streaming [both] [uplink] [downlink] x upgrade; } } </pre>
Hierarchy Level	[edit unified-edge cos-cac cos-policy-profiles <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the guaranteed bit rate (GBR) allowed for each traffic class. Optionally, you can configure the Broadband Gateway to allow bearers with a higher GBR than the configured value to be upgraded or rejected. You can configure different guaranteed bit rates for uplink and downlink traffic.
Options	<p>profile-name—Name of the CoS policy profile.</p> <p>Range: 1 through 256,000 Kbps.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring QoS on the Broadband Gateway Overview on page 323 • cos-policy-profiles on page 868

high

Syntax	<pre>high { gtpv1-arp y; gtpv2-priority-level z; percentage x; }</pre>
Hierarchy Level	[edit unified-edge cos-cac resource-threshold-profiles <i>name</i> system load bearer load cpu memory]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Set the high threshold level.
Options	<p><i>gtpv1-arp</i>—Designated (ARP) priority level.</p> <p><i>gtpv2-priority-level</i>—Designated priority level.</p> <p><i>percentage</i>—Percentage of the resource threshold to be increased.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring QoS on the Broadband Gateway Overview on page 323• bearer-load on page 861

inet-precedence

Syntax	<pre>inet-precedence <i>rewrite-rule-name</i> [protocol gtp-inet-both gtp-inet-outer];</pre>
Hierarchy Level	[edit class-of-service interfaces rewrite-rules]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Apply an IPv4 precedence rewrite rule. This rule is applied to packets going to the Packet Data Network (PDN).
Options	<i>rewrite-rule-name</i> —Name of the rewrite rule [gtp-inet-both gtp-inet-outer].
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring QoS on the Broadband Gateway Overview on page 323• rewrite-rules on page 889

inet-precedence (Ingress)

Syntax	<code>inet-precedence <i>rewrite-rule-name</i>;</code>
Hierarchy Level	[edit class-of-service interfaces ingress-rewrite-rules]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Apply an IPv4 precedence rewrite rule.
Options	<i>rewrite-rule-name</i> —Name of the rewrite rule [gtp-inet-both gtp-inet-outer].
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring QoS on the Broadband Gateway Overview on page 323 • ingress-rewrite-rules on page 875

ingress-rewrite-rules

Syntax	<pre>ingress-rewrite-rules { dscp <i>rewrite-rule-name</i>; dscp-ipv6 <i>rewrite-rule-name</i>; inet-precedence <i>rewrite-rule-name</i>; }</pre>
Hierarchy Level	[edit class-of-service interfaces]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure and apply ingress rewrite rules to the mobile interfaces under the CoS hierarchy within the IP header of upstream subscriber packets received on the mobile interface. This rule is applied to packets going to the core network.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring QoS on the Broadband Gateway Overview on page 323 • interfaces on page 876


interfaces

Syntax	<pre>interfaces { mif. number { rewrite-rules { dscp rewrite-rule-name [protocol gtp-inet-both gtp-inet-outer]; dscp-ipv6 rewrite-rule-name [protocol gtp-inet-both gtp-inet-outer]; inet-precedence rewrite-rule-name [protocol gtp-inet-both gtp-inet-outer]; } ingress-rewrite-rules { dscp rewrite-rule-name; dscp-ipv6 rewrite-rule-name; inet-precedence rewrite-rule-name; } } }</pre>
Hierarchy Level	[edit class-of-service]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Specify the mobile interfaces to set the CoS values for upstream and downstream subscriber packets.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring QoS on the Broadband Gateway Overview on page 323• class-of-service on page 864

local-policies

Syntax	<pre> local-policies { name { cos-policy-profile name; classifier-profile name; dl-bandwidth-pool name; roamer-classifier-profile name; roamer-cos-policy-profile name; resource-threshold-profiles name; ul-bandwidth-pool name; visitor-classifier-profile name; visitor-cos-policy-profile name; } } </pre>
Hierarchy Level	[edit unified-edge]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Define the quality of service (QoS) to be applied at the system level or APN level for a 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.</p>
Options	The remaining statements are explained separately.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring QoS on the Broadband Gateway Overview on page 323

local-policy-profile (Broadband Gateway)

Syntax	<code>local-policy-profile <i>local-policy-profile</i>;</code>
Hierarchy Level	[edit unified-edge gateways <i>ggsn-pgw gateway-name</i>], [edit unified-edge gateways <i>sgw gateway-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways <i>sgw name</i>] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Specify a local policy profile for the broadband gateway.</p> <ul style="list-style-type: none">For the broadband gateway configured as a gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW), the local policy profile is a combination of the quality-of-service (QoS) policy (cos-policy-profile), the classifier policy (classifier-profile), and the resource threshold policy (resource-threshold-policy).For the broadband gateway configured as a Serving Gateway (S-GW), the local policy profile is a combination of the classifier policy (classifier-profile) and the resource threshold policy (resource-threshold-policy).
	<div><p>NOTE: The local policy profile must already be configured at the [edit unified-edge] hierarchy level.</p></div>
Options	<i>local-policy-profile</i> —Name of the local policy profile.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">local-policy-profile (APN) on page 720 (P-GW only)

low

Syntax	<pre>low { gtpv1-arp y; gtpv2-priority-level z; percentage x; }</pre>
Hierarchy Level	[edit unified-edge cos-cac resource-threshold-profiles <i>name</i> system load bearer load cpu memory]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Set the low threshold level.
Options	<p><i>gtpv1-arp</i>—Designated (ARP) priority level.</p> <p><i>gtpv2-priority-level</i>—Designated priority level.</p> <p><i>percentage</i>—Percentage of the resource threshold to be lowered.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring QoS on the Broadband Gateway Overview on page 323 • bearer-load on page 861

maximum-bearers (Broadband Gateway)

Syntax	<code>maximum-bearers <i>maximum-bearers</i>;</code>
Hierarchy Level	[edit unified-edge gateways <i>ggsn-pgw gateway-name</i>], [edit unified-edge gateways <i>sgw gateway-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways <i>sgw name</i>] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>For the broadband gateway configured as a gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW), configure the maximum number of Evolved Packet System (EPS) bearers or packet data protocol (PDP) contexts allowed.</p> <p>For the broadband gateway configured as a Serving Gateway (S-GW), configure the maximum number of EPS bearers allowed.</p>
Options	<p><i>maximum-bearers</i>—Maximum number of bearers for the broadband gateway.</p> <p>Range: 100,000 through 12,000,000 bearers</p> <p>Default: 12,000,000 bearers</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Maximum Number of Bearers on page 324• maximum-bearers (APN) on page 722 (P-GW only)

maximum-bit-rate

Syntax	<pre>maximum-bit-rate { traffic-class-cos-policy-profiles { any [both] [uplink] [downlink] x background [both] [uplink] [downlink] x conversational [both] [uplink] [downlink] x interactive [both] [uplink] [downlink] x reject; streaming [both] [uplink] [downlink] x upgrade; } }</pre>
Hierarchy Level	[edit unified-edge cos-cac cos-policy-profiles <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the maximum bit rate (MBR) for each traffic class allowed. A bearer request that specifies a higher MBR than the configured 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.
Options	<p>The remaining statements are explained separately.</p> <p>Range: 1 through 256,000 Kbps.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring QoS on the Broadband Gateway Overview on page 323 • cos-policy-profiles on page 868


memory

Syntax	<pre>memory { low { gtpv1-arp y; gtpv2-priority-level z; percentage x; } high { gtpv1-arp y; gtpv2-priority-level z; percentage x; } }</pre>
Hierarchy Level	[edit unified-edge cos-cac resource-threshold-profiles <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the memory-load configuration. The memory load indicates a precise level of admission control when memory utilization reaches a configured lower or upper threshold.
Default	The bearer load is expressed as a percentage. If the bearer load is associated with the local policy the gateway low level is 70 percent and the gateway high level is 85 percent.
Options	<p><i>high</i>—High threshold configuration.</p> <p><i>low</i>—Low threshold configuration.</p> <p>Range: Low—70 percentHigh—85 percent</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring QoS on the Broadband Gateway Overview on page 323• resource-threshold-profiles on page 887


mif

Syntax	<pre> mif. number { rewrite-rules { dscp rewrite-rule-name [protocol gtp-inet-both gtp-inet-outer]; dscp-ipv6 rewrite-rule-name [protocol gtp-inet-both gtp-inet-outer]; inet-precedence rewrite-rule-name [protocol gtp-inet-both gtp-inet-outer]; } ingress-rewrite-rules { dscp rewrite-rule-name; dscp-ipv6 rewrite-rule-name; inet-precedence rewrite-rule-name; } } </pre>
Hierarchy Level	[edit class-of-service]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the mobile interface number to set the CoS values for upstream and downstream subscriber packets.
Options	The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring QoS on the Broadband Gateway Overview on page 323

preemption (GGSN or P-GW)

Syntax	<pre>preemption { enable; gtpv1-pci-disable; gtpv1-pvi-disable; }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure whether preemption should be enabled or disabled on the gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW). Preemption aids in call admission control and enables the gateway to accommodate higher priority bearers over the lower priority ones, based on the Preemption Capability Indicator (PCI) and Preemption Vulnerability Indicator (PVI).</p> <p>The PCI value defines whether a bearer with a lower priority level (PL) should be dropped to free the resources required. The PVI value defines whether a bearer is liable to be dropped in favor of a preemption-capable bearer with a higher priority level value.</p> <p>Preemption can be applied based on system, memory, CPU, and bearer load, and can be configured at the [edit unified-edge cos-cac resource-threshold-profiles] hierarchy level.</p> <div><p>NOTE: The <code>gtpv1-pci</code> and <code>gtpv1-pvi</code> values are valid only for General Packet Radio Service (GPRS) tunneling protocol version 1 (GTPv1) subscribers.</p></div>
Options	<p>enable—Enable preemption on the GGSN or P-GW. If you do not specify a value, preemption is disabled by default.</p> <p>gtpv1-pci-disable—Disable the preemption capability indicator for GTPv1 subscribers. If you do not specify a value, the preemption capability indicator is enabled by default.</p> <p>gtpv1-pvi-disable—Disable the preemption vulnerability indicator for GTPv1 subscribers. If you do not specify a value, the preemption vulnerability indicator is enabled by default.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Preemption for Call Admission Control on page 326

preemption (Serving Gateway)

Syntax	preemption { enable; }
Hierarchy Level	[edit unified-edge gateways <i>sgw gateway-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure whether preemption should be enabled or disabled on the Serving Gateway (S-GW). Preemption aids in call admission control and enables the gateway to accommodate higher priority bearers over the lower priority ones, based on the Preemption Capability Indicator (PCI) and Preemption Vulnerability Indicator (PVI).</p> <p>The PCI value defines whether a bearer with a lower priority level (PL) should be dropped to free the resources required. The PVI value defines whether a bearer is liable to be dropped in favor of a preemption-capable bearer with a higher priority level value.</p> <p>Preemption can be applied based on system, memory, CPU, and bearer load, and can be configured at the [edit unified-edge cos-cac resource-threshold-profiles] hierarchy level.</p> <div style="margin-top: 20px;">  <p>NOTE: In the S-GW, only bearers that are of the same type can preempt each other: guaranteed bit rate (GBR) bearers can preempt only GBR bearers, and non-GBR bearers can preempt only non-GBR bearers.</p> </div>
Default	If you do not configure this statement, preemption is disabled by default.
Options	enable —Enable preemption on the S-GW.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring an S-GW on a Broadband Gateway on page 30

qos-class-identifier

Syntax	<code>qci <x> forwarding-class <i>fc-name</i> loss-priority [low high];</code>
Hierarchy Level	[edit unified-edge cos-cac classifier-profiles <i>name</i>] [edit unified-edge cos-cac cos-policy-profiles <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the QCI mapping such as QCI values and associated QoS characteristics to the forwarding class and loss priority based on traffic requirements. The configuration directs the behavior for limiting, upgrading, or rejecting calls based on the requested maximum bit rate.
Options	<p><i>forwarding-class</i>—Forwarding class for handling packets on QoS.</p> <p><i>loss-priority</i>—Loss priority assigned to specific QoS values and aliases of the classifier profile.</p> <p>Range: 5 through 9</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring QoS on the Broadband Gateway Overview on page 323• cos-policy-profiles on page 868• classifier-profiles on page 863

resource-threshold-profiles

```
Syntax  resource-threshold-profiles {
        name {
            system-load {
                low {
                    gtpv1-arp y;
                    gtpv2-priority-level z;
                    percentage x;
                }
                high {
                    gtpv1-arp y;
                    gtpv2-priority-level z;
                    percentage x;
                }
            }
            bearer-load {
                low {
                    gtpv1-arp y;
                    gtpv2-priority-level z;
                    percentage x;
                }
                high {
                    gtpv1-arp y;
                    gtpv2-priority-level z;
                    percentage x;
                }
            }
            cpu {
                low {
                    gtpv1-arp y;
                    gtpv2-priority-level z;
                    percentage x;
                }
                high {
                    gtpv1-arp y;
                    gtpv2-priority-level z;
                    percentage x;
                }
            }
            memory {
                low {
                    gtpv1-arp y;
                    gtpv2-priority-level z;
                    percentage x;
                }
                high {
                    gtpv1-arp y;
                    gtpv2-priority-level z;
                    percentage x;
                }
            }
        }
    }
```

Hierarchy Level	[edit unified-edge cos-cac]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure a resource threshold profile to ensure that the bearer load, system load, CPU usage, or memory usage at the APN or system level on the broadband gateway reaches a specified threshold. On reaching the threshold, only bearer requests that meet or exceed a designated (ARP) priority level are accepted. A non-conforming traffic is either dropped or marked for preferential dropping when congestion occurs.
Options	<i>name</i> —Name of the resource threshold profile. The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring QoS on the Broadband Gateway Overview on page 323• cos-cac on page 865

resource-threshold-profile

Syntax	resource-threshold-profile <i>name</i> ;
Hierarchy Level	[edit unified-edge local-policies <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the limit for CPU and memory usage. When the number of bearers or system load reaches a configured low or high threshold, only higher-priority bearer requests are allowed. A load factors types such as bearer load, CPU load, memory load, generic system load, and so on. This configuration controls the behavior of the system on loaded condition. You may configure two thresholds, low or high, and each threshold must be associated with an allocation and retention priority.
Options	<i>name</i> —Name of the resource threshold profile.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring QoS on the Broadband Gateway Overview on page 323• local-policies on page 877

rewrite-rules

Syntax	<pre>rewrite-rules { dscp <i>rewrite-rule-name</i> [protocol gtp-inet-both gtp-inet-outer]; dscp-ipv6 <i>rewrite-rule-name</i> [protocol gtp-inet-both gtp-inet-outer]; inet-precedence <i>rewrite-rule-name</i> [protocol gtp-inet-both gtp-inet-outer]; }</pre>
Hierarchy Level	[edit class-of-service interfaces]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Associate the rewrite rules with the mobile interface. The rule is defined under the CoS hierarchy. You must configure and apply rewrite rules to set the value of the CoS bits within the IP header of downstream subscriber packets received on the mobile interface.
Options	The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring QoS on the Broadband Gateway Overview on page 323 • interfaces on page 876

roamer-classifier-profile

Syntax	roamer-classifier-profile <i>name</i> ;
Hierarchy Level	[edit unified-edge local-policies <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Define the mapping from the traffic class to the forwarding class (internal queues) and packet loss priority for roaming subscriber traffic.
Options	<i>name</i> —Name of the roamer classifier profile.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring QoS on the Broadband Gateway Overview on page 323 • local-policies on page 877

roamer-cos-policy-profile

Syntax	roamer-cos-policy-profile <i>name</i> ;
Hierarchy Level	[edit unified-edge local-policies <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Define policies for limiting, upgrading, or rejecting calls based on the requested QoS parameters specifically for roaming subscriber traffic.
Options	<i>name</i> —Name of the roamer CoS-policy profile.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring QoS on the Broadband Gateway Overview on page 323• local-policies on page 877

system-load

Syntax	<pre> system-load { low { gtpv1-arp y; gtpv2-priority-level z; percentage x; } high { gtpv1-arp y; gtpv2-priority-level z; percentage x; } } </pre>
Hierarchy Level	[edit unified-edge cos-cac resource-threshold-profiles <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the system load. The system load indicates a level of traffic flow control when memory utilization, CPU load, and queue depths (for GTP, RADIUS, and CDR) reach a configured lower or upper threshold.
Default	The bearer load is expressed as a percentage. If the bearer load is associated with the local policy, the gateway low level is 70 percent and the gateway high level is 85 percent.
Options	<p><i>high</i>—High threshold configuration.</p> <p><i>low</i>—Low threshold configuration.</p> <p>Range: Low—70 percent High—85 percent</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring QoS on the Broadband Gateway Overview on page 323 • resource-threshold-profiles on page 887

traffic-class-classifier-profiles

Syntax	<code>traffic-class conversational streaming background forwarding-class <i>forwarding-class-name</i> loss-priority [low high];</code> <code>traffic-class interactive traffic-handling-priority 1 2 3 forwarding-class <i>forwarding-class-name</i> loss-priority [low high];</code>
Hierarchy Level	[edit unified-edge cos-cac classifier-profiles <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the QoS classifier profile to define the traffic classes and map each traffic class to a forwarding class and packet loss priority in a 3G network. You may choose to configure among four traffic classes: conversational, streaming, interactive, and background. Configuring the appropriate options helps to manage traffic based on delay, jitter, bandwidth, and reliability.
Options	<p><i>background</i>—Name of the traffic classes alias.</p> <p><i>conversational</i>—Value of the code-point bits, in decimal form.</p> <p><i>forwarding-class loss-priority</i>—Forwarding class for handling packets on QoS. The loss priority is assigned to specific QoS values and aliases of the classifier profile.</p> <p><i>interactive</i>—Name of the traffic classes alias.</p> <p><i>streaming</i>—Value of the code-point bits, in decimal form.</p>
Required Privilege Level	<code>interface</code> —To view this statement in the configuration. <code>interface-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring QoS on the Broadband Gateway Overview on page 323• classifier-profiles on page 863

traffic-class-cos-policy-profiles

Syntax	traffic-class conversational streaming percentage <i>z downgrade</i> ;
Hierarchy Level	[edit unified-edge cos-cac cos-policy-profiles <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Any bearer setup with a traffic class or traffic handling priority that is above this value is, by default, downgraded. A Modify bearer request with a higher traffic class than the configured maximum traffic class is downgraded to maximum traffic class. Optionally, you can configure the broadband gateway to allow bearers with a lower traffic class to be upgraded or rejected
Options	<p><i>any</i>— Associated with uplink and downlink to the traffic class.</p> <p><i>background</i>—Name of the traffic classes alias. This is applicable to both uplink and downlink.</p> <p><i>conversational</i>—Value of the code-point bits, in decimal form. This is applicable to both uplink and downlink.</p> <p><i>interactive</i>—Name of the traffic classes alias. This is applicable to both uplink and downlink.</p> <p><i>reject</i>—Traffic class to be rejected.</p> <p><i>streaming</i>—Value of the code-point bits, in decimal form. This is applicable to both uplink and downlink.</p> <p><i>upgrade</i>—Traffic class to be upgraded.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring QoS on the Broadband Gateway Overview on page 323 • cos-policy-profiles on page 868

ul-bandwidth-pool

Syntax	<code>ul-bandwidth-pool <i>name</i> ;</code>
Hierarchy Level	<code>[edit unified-edge local-policies <i>name</i>]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the limit for uplink bandwidth usage at the system or APN level.
Options	<i>name</i> —Name of the uplink bandwidth pool.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring QoS on the Broadband Gateway Overview on page 323• local-policies on page 877

violate-action

Syntax	<code>violate-action [set-loss-priority-high transmit]</code>
Hierarchy Level	<code>[edit unified-edge cos-cac cos-policy-profiles <i>name</i>]</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Set the action to take when the specified levels for all the CoS policy profile parameters are exceeded.
Options	<i>set loss priority high</i> —Set the loss priority for violate action to high. <i>transmit</i> —Set the transmit levels for violate action.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring QoS on the Broadband Gateway Overview on page 323• cos-policy-profiles on page 868

visitor-classifier-profile

Syntax	visitor-classifier-profile <i>name</i> ;
Hierarchy Level	[edit unified-edge local-policies <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Define the mapping from the traffic class to the forwarding class (internal queues) and packet loss priority for visitor subscriber traffic.
Options	<i>name</i> —Name of the visitor classifier profile.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring QoS on the Broadband Gateway Overview on page 323 • local-policies on page 877

visitor-cos-policy-profile

Syntax	visitor-cos-policy-profile <i>name</i> ;
Hierarchy Level	[edit unified-edge local-policies <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Define policies for limiting, upgrading, or rejecting calls based on the requested QoS parameters specifically for visitor subscriber traffic.
Options	<i>name</i> —Name of the visitor CoS-policy profile.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring QoS on the Broadband Gateway Overview on page 323 • local-policies on page 877

Exception Handling Configuration Statements

current-hop-limit (IPv6 Router Advertisement)

Syntax	<code>current-hop-limit <i>current-hop-limit</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> ipv6-router-advertisement]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the value to be placed in the current-hop-limit field of the IPv6 router advertisement messages sent from the broadband gateway. This value is used as the hop limit in the outgoing IPv6 packets sent from the user equipment (UE).
Options	<p><i>current-hop-limit</i>—Current hop limit for the IPv6 router advertisement.</p> <p>Range: 0 through 3</p> <p>Default: 0. The hop limit is not specified by the broadband gateway.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring IPv6 Protocol Parameters on page 93 • Example: Configuring Broadband Gateway Exception Handling Parameters on page 99 • ipv6-router-advertisement (MobileNext Broadband Gateway) on page 901

disable (IPv6 Router Advertisement)

Syntax	disable;
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> ipv6-router-advertisement]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Disable IPv6 router advertisement for the broadband gateway. By default, IPv6 router advertisement is enabled for the broadband gateway.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring IPv6 Protocol Parameters on page 93• Example: Configuring Broadband Gateway Exception Handling Parameters on page 99• ipv6-router-advertisement (MobileNext Broadband Gateway) on page 901


error-indication-interval

Syntax	error-indication-interval <i>interval-in-seconds</i> ;
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> gtp data]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the interval at which the broadband gateway generates an error indication to the peer per bearer. One error indication is generated per bearer for the interval configured, in seconds.
Options	<i>interval-in-seconds</i> —Error indication interval. Range: 1 through 20 seconds Default: 2 seconds
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring GTP Services on the Data Plane on page 232• Example: Configuring Broadband Gateway Exception Handling Parameters on page 99• data (GTP) on page 920

ip-reassembly

Syntax	<pre>ip-reassembly <i>profile-name</i> { <i>max-reassembly-pending-packets</i> <i>number</i>; <i>timeout in-seconds</i>; }</pre>
Hierarchy Level	[edit services]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure an IP reassembly profile to be applied to the broadband gateway.</p> <p>The remaining statements are explained separately.</p>
Options	<i>profile-name</i> —Name of the IP reassembly profile.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Fragment Reassembly Parameters on page 90• Example: Configuring Broadband Gateway Exception Handling Parameters on page 99

ip-reassembly-profile

Syntax	<code>ip-reassembly-profile { <code>profile-name</code>; }</code>
Hierarchy Level	[edit unified-edge gateways <code>ggsn-pgw gateway-name</code>], [edit unified-edge gateways <code>sgw gateway-name</code>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways <code>sgw gateway-name</code>] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Apply a previously configured IP reassembly profile to the broadband gateway.
	<div><p>NOTE: Currently, only one IP reassembly profile is allowed for the broadband gateway.</p></div>
Options	<code>profile-name</code> —Name of the IP reassembly profile to be applied.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• [edit unified-edge gateways] Hierarchy Level on page 563• Configuring Fragment Reassembly Parameters on page 90• Example: Configuring Broadband Gateway Exception Handling Parameters on page 99

ipv6-router-advertisement (MobileNext Broadband Gateway)

Syntax	<pre> ipv6-router-advertisement { current-hop-limit <i>current-hop-limit</i>; disable; maximum-advertisement-interval <i>maximum-advertisement-interval</i>; maximum-initial-advertisement-interval <i>maximum-initial-advertisement-interval</i>; maximum-initial-advertisements <i>maximum-initial-advertisements</i>; minimum-advertisement-interval <i>minimum-advertisement-interval</i>; reachable-time <i>reachable-time</i>; retransmission-timer <i>retransmission-timer</i>; router-lifetime <i>router-lifetime</i>; } </pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure IPv6 router advertisement parameters for the broadband gateway.</p> <p>The remaining statements are explained separately.</p>
Default	By default, IPv6 router advertisement is enabled for the broadband gateway.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • [edit unified-edge gateways ggsn-pgw <gateway-name>] Hierarchy Level on page 564 • Configuring IPv6 Protocol Parameters on page 93 • Example: Configuring Broadband Gateway Exception Handling Parameters on page 99

max-reassembly-pending-packets (IP Reassembly)

Syntax	max-reassembly-pending-packets <i>number</i> ;
Hierarchy Level	[edit services ip-reassembly <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the maximum number of IPv4 packets pending reassembly that is allowed in each services PIC that belongs to the broadband gateway.
Options	<i>number</i> —Maximum number of packets pending reassembly allowed in each services PIC. Range: 100 through 10,000 Default: 2000
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Fragment Reassembly Parameters on page 90• Example: Configuring Broadband Gateway Exception Handling Parameters on page 99• ip-reassembly on page 899

maximum-advertisement-interval (IPv6 Router Advertisement)

Syntax	maximum-advertisement-interval <i>maximum-advertisement-interval</i> ;
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> ipv6-router-advertisement]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the maximum interval between unsolicited router advertisements.</p> <p>Router advertisements occur in phases. In the initial phase, the interval between the router advertisements is a few seconds. In the later phases, the interval increases to a few minutes. The maximum-advertisement-interval parameter controls the interval in the later phases.</p>
Options	<p>maximum-advertisement-interval—Maximum interval between unsolicited router advertisements.</p> <p>Range: 5400 through 21,600 seconds</p> <p>Default: 21,600 seconds</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring IPv6 Protocol Parameters on page 93 • Example: Configuring Broadband Gateway Exception Handling Parameters on page 99 • ipv6-router-advertisement (MobileNext Broadband Gateway) on page 901

maximum-initial-advertisement-interval (IPv6 Router Advertisement)

Syntax	<code>maximum-initial-advertisement-interval <i>maximum-initial-advertisement-interval</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> ipv6-router-advertisement]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the maximum interval between initial router advertisements.</p> <p>Router advertisements occur in phases. In the initial phase, the interval between the router advertisements is a few seconds. In the later phases, the interval increases to a few minutes. The maximum-initial-advertisement-interval parameter controls the interval in the initial phase.</p>
Options	<p><i>maximum-initial-advertisement-interval</i>—Maximum interval between initial router advertisements.</p> <p>Range: 10 through 16 seconds</p> <p>Default: 10 seconds</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring IPv6 Protocol Parameters on page 93• Example: Configuring Broadband Gateway Exception Handling Parameters on page 99• ipv6-router-advertisement (MobileNext Broadband Gateway) on page 901

maximum-initial-advertisements (IPv6 Router Advertisement)

Syntax	<code>maximum-initial-advertisements</code> <i>maximum-initial-advertisements</i> ;
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> ipv6-router-advertisement]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the maximum number of router advertisements sent during the initial phase.</p> <p>Router advertisements occur in phases. In the initial phase, the router advertisements occur every few seconds. In the later phases, the advertisements occur every few minutes. The maximum-initial-advertisements parameter controls the maximum number of advertisements sent during the initial phase.</p>
Options	<p><i>maximum-initial-advertisements</i>—Maximum number of initial router advertisements.</p> <p>Range: 2 through 5</p> <p>Default: 3</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring IPv6 Protocol Parameters on page 93 • Example: Configuring Broadband Gateway Exception Handling Parameters on page 99 • ipv6-router-advertisement (MobileNext Broadband Gateway) on page 901

minimum-advertisement-interval (IPv6 Router Advertisement)

Syntax	<code>minimum-advertisement-interval <i>minimum-advertisement-interval</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> ipv6-router-advertisement]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the minimum time allowed between the sending of unsolicited router advertisements.</p> <p>Router advertisements occur in phases. In the initial phase, the interval between the router advertisements is a few seconds. In the later phases, the interval increases to a few minutes. The minimum-advertisement-interval parameter controls the interval in the later phases.</p>
Options	<p><i>minimum-advertisement-interval</i>—Minimum interval between unsolicited router advertisements.</p> <p>Range: 3600 through 16,200 seconds</p> <p>Default: 16,200 seconds</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring IPv6 Protocol Parameters on page 93• Example: Configuring Broadband Gateway Exception Handling Parameters on page 99• ipv6-router-advertisement (MobileNext Broadband Gateway) on page 901

reachable-time (IPv6 Router Advertisement)

Syntax	<code>reachable-time <i>reachable-time</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> ipv6-router-advertisement]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the value of the reachable time field of IPv6 router advertisement messages. This is the time (in milliseconds) after which a node (user equipment [UE]) assumes that a neighbor is unreachable after the node had received the initial reachability confirmation. Because the GPRS tunneling protocol (GTP) tunnel behaves like a point-to-point IPv6 link between the user equipment and the gateway, the neighbor for the user equipment is usually the broadband gateway.
Options	<p><i>reachable-time</i>—Value of the reachable time field of the IPv6 router advertisement messages.</p> <p>Range: 0 through 3,600,000 milliseconds</p> <p>Default: 0 milliseconds. The reachable time has not been specified by the broadband gateway.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring IPv6 Protocol Parameters on page 93 • Example: Configuring Broadband Gateway Exception Handling Parameters on page 99 • ipv6-router-advertisement (MobileNext Broadband Gateway) on page 901

retransmission-timer (IPv6 Router Advertisement)

Syntax	<code>retransmission-timer <i>retransmission-timer</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> ipv6-router-advertisement]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the value of the retransmission timer field of the IPv6 router advertisement messages. The retransmission timer is used to control the time (in milliseconds) between retransmissions of neighbor solicitation messages from the user equipment (UE).
Options	<p><i>retransmission-timer</i>—Value of the retransmission timer field of the IPv6 router advertisement messages</p> <p>Default: 0 milliseconds. The retransmission timer has not been specified by the broadband gateway.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring IPv6 Protocol Parameters on page 93• Example: Configuring Broadband Gateway Exception Handling Parameters on page 99• ipv6-router-advertisement (MobileNext Broadband Gateway) on page 901

router-lifetime (IPv6 Router Advertisement)

Syntax	<code>router-lifetime <i>router-lifetime</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> ipv6-router-advertisement]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the value of the router lifetime field of the IPv6 router advertisement messages. The router-lifetime indicates the maximum time up to which the broadband gateway can be considered the default gateway.
Options	<p>router-lifetime—Value of the router lifetime field of the IPv6 router advertisement messages.</p> <p>Range: 5400 through 21,840 seconds</p> <p>Default: 21,840 seconds</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring IPv6 Protocol Parameters on page 93 • Example: Configuring Broadband Gateway Exception Handling Parameters on page 99 • ipv6-router-advertisement (MobileNext Broadband Gateway) on page 901

software-datapath

Syntax	<pre>software-datapath { traceoptions { file <i>filename</i> { files <i>files</i>; match <i>match</i>; size <i>size</i>; (no-world-readable world-readable); } flag { <i>flag</i>; } level <i>level</i>; no-remote-trace; } }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i>], [edit unified-edge gateways sgw <i>gateway-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i>] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Specify the configuration for the software datapath. The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• [edit unified-edge gateways] Hierarchy Level on page 563• Configuring Exception Handling Traceoptions on page 95

timeout (IP Reassembly)

Syntax	timeout <i>in-seconds</i> ;
Hierarchy Level	[edit services ip-reassembly <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the maximum time to wait for all IPv4 fragments of a packet to arrive for reassembly.
Options	<i>in-seconds</i> —Timeout for the fragments arriving for reassembly. Range: 2 through 60 seconds Default: 4 seconds
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Fragment Reassembly Parameters on page 90• Example: Configuring Broadband Gateway Exception Handling Parameters on page 99• ip-reassembly on page 899

traceoptions (Exception Handling)

Syntax	<pre>traceoptions { file <i>filename</i> { files <i>files</i>; match <i>match</i>; size <i>size</i>; (no-world-readable world-readable); } flag { <i>flag</i>; } level <i>level</i>; no-remote-trace; }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> software-datapath], [edit unified-edge gateways sgw <i>gateway-name</i> software datapath]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> software-datapath] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Define tracing operations for exception handling.
Options	<p>file <i>filename</i>—Name of the file that receives the output of the tracing operation. All files are placed in the /var/log directory.</p> <p>files <i>files</i>— (Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you must also specify a maximum file size with the size option and a filename.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag</p> <ul style="list-style-type: none">• <i>flag</i>—You can use one of the following flags:<ul style="list-style-type: none">• ager—Trace flow ageout-related events.• all—Trace everything.• buffering—Trace buffering.• commands—Trace operational commands.• configuration—Trace configuration commands.• flow—Trace flow.

- **init**—Trace events related to the **init** datapath daemon .
- **ipv6-router-advertisement**—Trace IPv6 router advertisements.
- **memory**—Trace memory.
- **reassembly**—Trace reassembly.
- **redundancy**—Trace redundancy.

level *level*—(Optional) Level of tracing to perform. You can specify any of the following levels:

- **all**—Match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match conditions that should be handled specially.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

match *match*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—(Optional) Disable remote tracing.

no-world-readable—(Optional) Restrict access to the originator of the trace operation only.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you must also specify a maximum number of trace files with the **files** option and filename.

Syntax: **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Exception Handling Traceoptions on page 95 • software-datapath on page 910

Gateway Maintenance Mode Configuration Statement

service-mode (GGSN or P-GW)

Syntax	service-mode maintenance;
Hierarchy Level	[edit unified-edge gateways <i>ggsn-pgw gateway-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>This statement puts the respective gateway under maintenance mode.</p> <p>When you have to make the following changes to the existing gateway configuration, you must put that gateway under maintenance mode:</p> <ul style="list-style-type: none">• Deleting certain GTP interfaces, such as Gn, Gp, S5, and S8• Changing the GTP interface address• Deleting the gateway
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• ggsn-pgw on page 986• Mobility Maintenance Mode Overview on page 394

service-mode (Serving Gateway)

Syntax	<code>service-mode service-mode-options;</code>
Hierarchy Level	[edit unified-edge gateways <i>sgw gateway-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	<p>Specify that the Serving Gateway (S-GW) should be in maintenance mode. You do this if you want to perform maintenance tasks such as deleting certain GTP parameters or modifying the GTP interface address on the S-GW. See the <i>MobileNext Broadband Gateway Configuration Guide</i> for a list of maintenance tasks that you can perform when the S-GW is in maintenance mode.</p> <p>When in the Maintenance Mode Active Phase, you can modify all valid attributes on the object. In all other cases, you can modify only the non-maintenance mode attributes.</p>
Options	service-mode-options —Specify the service mode. Currently, only the maintenance mode is option supported.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• sgw on page 998• show unified-edge sgw service-mode on page 1284

GTP Configuration Statements

control (GTP)

Syntax	<pre>control { ddn-delay-sync (disable enable); #S-GW only dscp-code-point <i>value</i>; echo-interval <i>interval</i>; echo-n3-requests <i>requests</i>; echo-t3-response <i>response-interval</i>; forwarding-class <i>class-name</i>; interface { <i>interface-name</i>; v4-address <i>v4-address</i>; } n3-requests <i>requests</i>; no-response-cache; path-management (disable enable); response-cache-timeout <i>interval-in-seconds</i>; t3-response <i>response-interval</i>; t1-value <i>t1-value</i>; #S-GW only }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>name</i> gtp], [edit unified-edge gateways sgw <i>name</i> gtp]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw gateway-name gtp] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the path and tunnel management parameters for the control plane. This configuration overrides the parameters configured at a higher hierarchy level.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring GTP Services Overview on page 226 • gtp (GGSN or P-GW) on page 936 • gtp (S-GW) on page 941

control (GTP Gn, Gp, S4, S5, and S8 Interfaces)

Syntax	<pre>control { dscp-code-point <i>value</i>; echo-interval <i>interval</i>; echo-n3-requests <i>requests</i>; echo-t3-response <i>response-interval</i>; forwarding-class <i>class-name</i>; interface { interface-name; v4-address <i>v4-address</i>; } n3-requests <i>requests</i>; path-management (disable enable); support-16-bit-sequence; #P-GW: S5 and S8 only t3-response <i>response-interval</i>; ttl-value <i>ttl-value</i>; #S-GW: S4, S5, and S8 only }</pre>
Hierarchy Level	<p>[edit unified-edge gateways ggsn-pgw <i>name</i> gtp gn], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp gp], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s5], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s8], [edit unified-edge gateways sgw <i>name</i> gtp s4], [edit unified-edge gateways sgw <i>name</i> gtp s5], [edit unified-edge gateways sgw <i>name</i> gtp s8]</p>
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W. Support at the following hierarchy levels introduced in Junos OS Mobility Release 11.4W:</p> <ul style="list-style-type: none"> • [edit unified-edge gateways sgw <i>gateway-name</i> gtp s4] hierarchy level • [edit unified-edge gateways sgw <i>gateway-name</i> gtp s5] hierarchy level • [edit unified-edge gateways sgw <i>gateway-name</i> gtp s8] hierarchy level
Description	<p>Configure the path and tunnel management parameters for the control plane for the Gn, Gp, S4, S5, or S8 interfaces. This configuration overrides the parameters configured at a higher hierarchy level.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring GTP Services Overview on page 226 • gn on page 932 • gp on page 934 • s4 on page 960 • s5 on page 962

- [s8 on page 964](#)

control (Peer Group)

Syntax	control { support-16-bit-sequence ; }
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>name</i> gtp peer-group <i>peer-group</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure support for 16-bit sequence numbers for interoperation with older gateways that support a GTP version with a 16-bit sequence number length. The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring GTP Services Overview on page 226 • peer-group (GTP) on page 953

data (GTP)

Syntax	<pre>data { echo-interval <i>interval</i>; echo-n3-requests <i>requests</i>; echo-t3-response <i>response-interval</i>; error-indication-interval <i>seconds</i>; indirect-tunnel (disable enable); #S-GW only interface { interface-name; v4-address <i>v4-address</i>; } num-gtpu-end-markers <i>num-gtpu-end-markers</i>; #S-GW only path-management (disable enable); }</pre>
Hierarchy Level	[edit unified-edge gateways <i>ggsn-pgw name gtp</i>], [edit unified-edge gateways <i>sgw name gtp</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways <i>sgw gateway-name gtp</i>] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the path and tunnel management parameters for the data plane. This configuration overrides the parameters configured at a higher hierarchy level.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring GTP Services Overview on page 226• gtp (GGSN or P-GW) on page 936• gtp (S-GW) on page 941

data (GTP Gn, Gp, S4, S5, and S8 Interfaces)

Syntax	<pre> data { echo-interval <i>interval</i>; echo-n3-requests <i>requests</i>; echo-t3-response <i>response-interval</i>; interface { interface-name; v4-address <i>v4-address</i>; } n3-requests <i>requests</i>; #P-GW only path-management (disable enable); t3-response <i>response-interval</i>; #P-GW only } </pre>
Hierarchy Level	<p>[edit unified-edge gateways ggsn-pgw <i>name</i> gtp gn], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp gp], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s5], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s8], [edit unified-edge gateways sgw <i>name</i> gtp s4], [edit unified-edge gateways sgw <i>name</i> gtp s5], [edit unified-edge gateways sgw <i>name</i> gtp s8]</p>
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W. Support at the following hierarchy levels introduced in Junos OS Mobility Release 11.4W:</p> <ul style="list-style-type: none"> • [edit unified-edge gateways sgw <i>gateway-name</i> gtp s4] hierarchy level • [edit unified-edge gateways sgw <i>gateway-name</i> gtp s5] hierarchy level • [edit unified-edge gateways sgw <i>gateway-name</i> gtp s8] hierarchy level
Description	<p>Configure the path and tunnel management parameters for the data plane for the Gn, Gp, S4, S5, or S8 interfaces. This configuration overrides the parameters configured at a higher hierarchy level.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring GTP Services Overview on page 226 • gn on page 932 • gp on page 934 • s4 on page 960 • s5 on page 962 • s8 on page 964

ddn-delay-sync

Syntax	<code>ddn-delay-sync (disable enable);</code>
Hierarchy Level	[edit unified-edge gateways <i>sgw gateway-name</i> gtp control]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Specify whether the synchronizing of the Downlink Data Notification (DDN) delay value with the other services PICs on the Serving Gateway should be disabled or enabled. DDN delay value synchronization is enabled by default.
Options	disable —Disable DDN delay value synchronization. enable —Enable DDN delay value synchronization.
Required Privilege Level	interface —To view this statement in the configuration. interface-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring General GTP Service on the S-GW on page 249• control (GTP) on page 917

dscp-code-point (GTP)

Syntax	<code>dscp-code-point <i>value</i>;</code>
Hierarchy Level	<p>[edit unified-edge gateways ggsn-pgw <i>name</i> gtp control], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp gn control], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp gp control], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s5 control], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s8 control], [edit unified-edge gateways sgw <i>name</i> gtp control], [edit unified-edge gateways sgw <i>name</i> gtp s11], [edit unified-edge gateways sgw <i>name</i> gtp s4 control], [edit unified-edge gateways sgw <i>name</i> gtp s5 control], [edit unified-edge gateways sgw <i>name</i> gtp s8 control]</p>
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W. Support at the following hierarchy levels introduced in Junos OS Mobility Release 11.4W:</p> <ul style="list-style-type: none"> • [edit unified-edge gateways sgw <i>name</i> gtp control] • [edit unified-edge gateways sgw <i>name</i> gtp s11] • [edit unified-edge gateways sgw <i>name</i> gtp s4 control] • [edit unified-edge gateways sgw <i>name</i> gtp s5 control] • [edit unified-edge gateways sgw <i>name</i> gtp s8 control]
Description	Specify the value of the Differentiated Services (DiffServ) field within the IP header. DiffServ code point (DSCP) is used exclusively for GTP messages.
Options	<i>value</i> —DSCP value.
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring GTP Services Overview on page 226 • control (GTP) on page 917

echo-interval (GTP)

Syntax `echo-interval interval;`

Hierarchy Level [edit unified-edge gateways ggsn-pgw *name* gtp],
[edit unified-edge gateways ggsn-pgw *name* gtp control],
[edit unified-edge gateways ggsn-pgw *name* gtp data],
[edit unified-edge gateways ggsn-pgw *name* gtp gn],
[edit unified-edge gateways ggsn-pgw *name* gtp gn control],
[edit unified-edge gateways ggsn-pgw *name* gtp gn data],
[edit unified-edge gateways ggsn-pgw *name* gtp gp],
[edit unified-edge gateways ggsn-pgw *name* gtp gp control],
[edit unified-edge gateways ggsn-pgw *name* gtp gp data],
[edit unified-edge gateways ggsn-pgw *name* gtp peer-group *name*],
[edit unified-edge gateways ggsn-pgw *name* gtp s5],
[edit unified-edge gateways ggsn-pgw *name* gtp s5 control],
[edit unified-edge gateways ggsn-pgw *name* gtp s5 data],
[edit unified-edge gateways ggsn-pgw *name* gtp s8],
[edit unified-edge gateways ggsn-pgw *name* gtp s8 control],
[edit unified-edge gateways ggsn-pgw *name* gtp s8 data],
[edit unified-edge gateways sgw *name* gtp],
[edit unified-edge gateways sgw *name* gtp control],
[edit unified-edge gateways sgw *name* gtp data],
[edit unified-edge gateways sgw *name* gtp s11],
[edit unified-edge gateways sgw *name* gtp s12],
[edit unified-edge gateways sgw *name* gtp s1u],
[edit unified-edge gateways sgw *name* gtp s4],
[edit unified-edge gateways sgw *name* gtp s4 control],
[edit unified-edge gateways sgw *name* gtp s4 data],
[edit unified-edge gateways sgw *name* gtp s5],
[edit unified-edge gateways sgw *name* gtp s5 control],
[edit unified-edge gateways sgw *name* gtp s5 data],
[edit unified-edge gateways sgw *name* gtp s8],
[edit unified-edge gateways sgw *name* gtp s8 control],
[edit unified-edge gateways sgw *name* gtp s8 data]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.
Support at the following hierarchy levels introduced in Junos OS Mobility Release 11.4W:

- [edit unified-edge gateways sgw *name* gtp]
- [edit unified-edge gateways sgw *name* gtp control]
- [edit unified-edge gateways sgw *name* gtp data]
- [edit unified-edge gateways sgw *name* gtp s11]
- [edit unified-edge gateways sgw *name* gtp s12]
- [edit unified-edge gateways sgw *name* gtp s1u],
- [edit unified-edge gateways sgw *name* gtp s4]
- [edit unified-edge gateways sgw *name* gtp s4 control]
- [edit unified-edge gateways sgw *name* gtp s4 data]

- [edit unified-edge gateways *sgw name* gtp s5]
- [edit unified-edge gateways *sgw name* gtp s5 control]
- [edit unified-edge gateways *sgw name* gtp s5 data]
- [edit unified-edge gateways *sgw name* gtp s8]
- [edit unified-edge gateways *sgw name* gtp s8 control]
- [edit unified-edge gateways *sgw name* gtp s8 data]

Description Configure the echo request interval for path management.

- For the Gateway GPRS Support Node (GGSN) or Packet Data Network Gateway (P-GW), the echo request interval is the number of seconds that the GGSN or P-GW waits before sending an echo request message to its peer (SGSN or S-GW).
- For the Serving Gateway (S-GW), the echo request interval is the number of seconds that the S-GW waits before sending an echo request message to its peer (MME, S4-SGSN, or P-GW).

This interval applies to both GTP-C and GTP-U echo messages.

Options *interval*—Echo request interval, in seconds.

Range: 60 through 65535 seconds.

Default: 60 seconds.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [GTP Path Management Overview on page 216](#)
- [gtp \(GGSN or P-GW\) on page 936](#)
- [gtp \(S-GW\) on page 941](#)

echo-n3-requests

Syntax `echo-n3-requests requests;`

Hierarchy Level [edit unified-edge gateways ggsn-pgw *name* gtp],
[edit unified-edge gateways ggsn-pgw *name* gtp control],
[edit unified-edge gateways ggsn-pgw *name* gtp data],
[edit unified-edge gateways ggsn-pgw *name* gtp gn],
[edit unified-edge gateways ggsn-pgw *name* gtp gn control],
[edit unified-edge gateways ggsn-pgw *name* gtp gn data],
[edit unified-edge gateways ggsn-pgw *name* gtp gp],
[edit unified-edge gateways ggsn-pgw *name* gtp gp control],
[edit unified-edge gateways ggsn-pgw *name* gtp gp data],
[edit unified-edge gateways ggsn-pgw *name* gtp peer-group *name*],
[edit unified-edge gateways ggsn-pgw *name* gtp s5],
[edit unified-edge gateways ggsn-pgw *name* gtp s5 control],
[edit unified-edge gateways ggsn-pgw *name* gtp s5 data],
[edit unified-edge gateways ggsn-pgw *name* gtp s8],
[edit unified-edge gateways ggsn-pgw *name* gtp s8 control],
[edit unified-edge gateways ggsn-pgw *name* gtp s8 data],
[edit unified-edge gateways sgw *name* gtp],
[edit unified-edge gateways sgw *name* gtp control],
[edit unified-edge gateways sgw *name* gtp data],
[edit unified-edge gateways sgw *name* gtp s11],
[edit unified-edge gateways sgw *name* gtp s12],
[edit unified-edge gateways sgw *name* gtp s1u],
[edit unified-edge gateways sgw *name* gtp s4],
[edit unified-edge gateways sgw *name* gtp s4 control],
[edit unified-edge gateways sgw *name* gtp s4 data],
[edit unified-edge gateways sgw *name* gtp s5],
[edit unified-edge gateways sgw *name* gtp s5 control],
[edit unified-edge gateways sgw *name* gtp s5 data],
[edit unified-edge gateways sgw *name* gtp s8],
[edit unified-edge gateways sgw *name* gtp s8 control],
[edit unified-edge gateways sgw *name* gtp s8 data]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.
Support at the following hierarchy levels introduced in Junos OS Mobility Release 11.4W:

- [edit unified-edge gateways sgw *name* gtp]
- [edit unified-edge gateways sgw *name* gtp control]
- [edit unified-edge gateways sgw *name* gtp data]
- [edit unified-edge gateways sgw *name* gtp s11]
- [edit unified-edge gateways sgw *name* gtp s12]
- [edit unified-edge gateways sgw *name* gtp s1u]
- [edit unified-edge gateways sgw *name* gtp s4]
- [edit unified-edge gateways sgw *name* gtp s4 control]
- [edit unified-edge gateways sgw *name* gtp s4 data]

- [edit unified-edge gateways *sgw name* gtp s5]
- [edit unified-edge gateways *sgw name* gtp s5 control]
- [edit unified-edge gateways *sgw name* gtp s5 data]
- [edit unified-edge gateways *sgw name* gtp s8]
- [edit unified-edge gateways *sgw name* gtp s8 control]
- [edit unified-edge gateways *sgw name* gtp s8 data]

Description Configure the maximum number of retries of GTP echo request messages for path management. Echo request messages are resent only when there is no response to the transmitted echo request messages within the configured response timeout value (for GTP echo request messages).

Options *requests*—Maximum number of times that the broadband gateway attempts to send an echo request message.

Range: 1 through 5

Default: 3

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring GTP Services Overview on page 226](#)
- [gtp \(GGSN or P-GW\) on page 936](#)
- [gtp \(S-GW\) on page 941](#)

echo-t3-response

Syntax `echo-t3-response response-interval;`

Hierarchy Level [edit unified-edge gateways ggsn-pgw *name* gtp],
[edit unified-edge gateways ggsn-pgw *name* gtp control],
[edit unified-edge gateways ggsn-pgw *name* gtp data],
[edit unified-edge gateways ggsn-pgw *name* gtp gn],
[edit unified-edge gateways ggsn-pgw *name* gtp gn control],
[edit unified-edge gateways ggsn-pgw *name* gtp gn data],
[edit unified-edge gateways ggsn-pgw *name* gtp gp],
[edit unified-edge gateways ggsn-pgw *name* gtp gp control],
[edit unified-edge gateways ggsn-pgw *name* gtp gp data],
[edit unified-edge gateways ggsn-pgw *name* gtp peer-group *name*],
[edit unified-edge gateways ggsn-pgw *name* gtp s5],
[edit unified-edge gateways ggsn-pgw *name* gtp s5 control],
[edit unified-edge gateways ggsn-pgw *name* gtp s5 data],
[edit unified-edge gateways ggsn-pgw *name* gtp s8],
[edit unified-edge gateways ggsn-pgw *name* gtp s8 control],
[edit unified-edge gateways ggsn-pgw *name* gtp s8 data],
[edit unified-edge gateways sgw *name* gtp],
[edit unified-edge gateways sgw *name* gtp control],
[edit unified-edge gateways sgw *name* gtp data],
[edit unified-edge gateways sgw *name* gtp s11],
[edit unified-edge gateways sgw *name* gtp s12],
[edit unified-edge gateways sgw *name* gtp s1u],
[edit unified-edge gateways sgw *name* gtp s4],
[edit unified-edge gateways sgw *name* gtp s4 control],
[edit unified-edge gateways sgw *name* gtp s4 data],
[edit unified-edge gateways sgw *name* gtp s5],
[edit unified-edge gateways sgw *name* gtp s5 control],
[edit unified-edge gateways sgw *name* gtp s5 data],
[edit unified-edge gateways sgw *name* gtp s8],
[edit unified-edge gateways sgw *name* gtp s8 control],
[edit unified-edge gateways sgw *name* gtp s8 data]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.
Support at the following hierarchy levels introduced in Junos OS Mobility Release 11.4W:

- [edit unified-edge gateways sgw *name* gtp]
- [edit unified-edge gateways sgw *name* gtp control],
- [edit unified-edge gateways sgw *name* gtp data]
- [edit unified-edge gateways sgw *name* gtp s11]
- [edit unified-edge gateways sgw *name* gtp s12]
- [edit unified-edge gateways sgw *name* gtp s1u]
- [edit unified-edge gateways sgw *name* gtp s4]
- [edit unified-edge gateways sgw *name* gtp s4 control]
- [edit unified-edge gateways sgw *name* gtp s4 data]

- [edit unified-edge gateways *sgw name* gtp s5]
- [edit unified-edge gateways *sgw name* gtp s5 control]
- [edit unified-edge gateways *sgw name* gtp s5 data]
- [edit unified-edge gateways *sgw name* gtp s8]
- [edit unified-edge gateways *sgw name* gtp s8 control]
- [edit unified-edge gateways *sgw name* gtp s8 data]

Description	Configure the response timeout for a GTP echo request message. The response timeout indicates the time (in seconds) that the broadband gateway waits before transmitting the next echo request message if it does not receive a response.
Default	If you do not include this statement, the response timeout is set to 5 seconds.
Options	<i>response interval</i> —Time, in seconds, that the gateway waits before transmitting the next echo request message if it does not receive a response. Range: 1 through 65,535 seconds Default: 15 seconds
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring GTP Services Overview on page 226• gtp (GGSN or P-GW) on page 936• gtp (S-GW) on page 941

error-indication-interval

Syntax	<code>error-indication-interval <i>seconds</i>;</code>
Hierarchy Level	[edit unified-edge gateways <i>ggsn-pgw name</i> gtp data], [edit unified-edge gateways <i>ggsn-pgw name</i> gtp s8 data], [edit unified-edge gateways <i>sgw name</i> gtp data], [edit unified-edge gateways <i>sgw name</i> gtp s8 data]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the interval at which the broadband gateway generates an error indication (Tunnel Endpoint Identifier [TEID] error message) to the peer per bearer. One error indication is generated per bearer for the interval configured, in seconds.
Options	<i>seconds</i> — Number of seconds that the gateway waits before indicating an error message to the peer. Range: 1 through 20 seconds Default: 2 seconds
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring GTP Services Overview on page 226• gtp (GGSN or P-GW) on page 936• gtp (S-GW) on page 941

forwarding-class (GTP)

Syntax	<code>forwarding-class <i>class-name</i>;</code>
Hierarchy Level	<p>[edit unified-edge gateways ggsn-pgw <i>name</i> gtp control], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp gn control], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp gp control], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s5 control], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s8 control], [edit unified-edge gateways sgw <i>name</i> gtp control], [edit unified-edge gateways sgw <i>name</i> gtp s4 control], [edit unified-edge gateways sgw <i>name</i> gtp s5 control], [edit unified-edge gateways sgw <i>name</i> gtp s8 control]</p>
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W. Support at the following hierarchy levels introduced in Junos OS Mobility Release 11.4W:</p> <ul style="list-style-type: none"> • [edit unified-edge gateways sgw <i>name</i> gtp control] • [edit unified-edge gateways sgw <i>name</i> gtp s4 control] • [edit unified-edge gateways sgw <i>name</i> gtp s5 control] • [edit unified-edge gateways sgw <i>name</i> gtp s8 control]
Description	Specify a forwarding class for outbound control packets.
Options	<i>class-name</i> —Name of the forwarding class.
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring GTP Services Overview on page 226 • control (GTP) on page 917

gn

```
Syntax  gn {
        control {
            dscp-code-point value;
            echo-interval interval;
            echo-n3-requests requests;
            echo-t3-response response-interval;
            forwarding-class class-name;
            interface {
                interface-name;
                v4-address v4-address;
            }
            n3-requests requests;
            path-management (disable | enable);
            t3-response response-interval;
        }
        data {
            echo-interval interval;
            echo-n3-requests requests;
            echo-t3-response response-interval;
            interface {
                interface-name;
                v4-address v4-address;
            }
            n3-requests requests;
            path-management (disable | enable);
            t3-response response-interval;
        }
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        interface {
            interface-name;
            v4-address v4-address;
        }
        n3-requests requests;
        path-management (disable | enable);
        t3-response response-interval;
    }
```

Hierarchy Level [edit unified-edge gateways ggsn-pgw *name* gtp]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the path and tunnel management parameters for the 3GPP Gn interface. This configuration overrides the parameters configured at a higher level in the hierarchy and applies to all GTP peers that connect to the Gn interface. You can also configure parameters only for GTP control packets or GTP user plane packets—these parameters override the parameters at the higher hierarchy levels.

The remaining statements are explained separately.

Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring GTP Services Overview on page 226• gtp (GGSN or P-GW) on page 936• gtp (S-GW) on page 941

gp

```
Syntax  gp {
        control {
            dscp-code-point value;
            echo-interval interval;
            echo-n3-requests requests;
            echo-t3-response response-interval;
            forwarding-class class-name;
            interface {
                interface-name;
                v4-address v4-address;
            }
            n3-requests requests;
            path-management (disable | enable);
            t3-response response-interval;
        }
        data {
            echo-interval interval;
            echo-n3-requests requests;
            echo-t3-response response-interval;
            interface {
                interface-name;
                v4-address v4-address;
            }
            n3-requests requests;
            path-management (disable | enable);
            t3-response response-interval;
        }
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        interface {
            interface-name;
            v4-address v4-address;
        }
        n3-requests requests;
        path-management (disable | enable);
        t3-response response-interval;
    }
```

Hierarchy Level [edit unified-edge gateways ggsn-pgw *name* gtp]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the path and tunnel management parameters for the 3GPP Gp interface. This configuration overrides the parameters configured at a higher level in the hierarchy and applies to all GTP peers that connect to the Gp interface. You can also configure parameters only for GTP control packets or GTP user plane packets—these parameters override the parameters at the higher hierarchy levels.

The remaining statements are explained separately.

Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring GTP Services Overview on page 226• gtp (GGSN or P-GW) on page 936• gtp (S-GW) on page 941

gtp (GGSN or P-GW)

```
Syntax  gtp {
        control {
            dscp-code-point value;
            echo-interval interval;
            echo-n3-requests requests;
            echo-t3-response response-interval;
            forwarding-class class-name;
            interface {
                interface-name;
                v4-address v4-address;
            }
            n3-requests requests;
            no-response-cache;
            path-management (disable | enable);
            response-cache-timeout t interval-in-seconds;
            t3-response response-interval;
        }
        data {
            echo-interval interval;
            echo-n3-requests requests;
            echo-t3-response response-interval;
            error-indication-interval seconds;
            interface {
                interface-name;
                v4-address v4-address;
            }
            path-management (disable | enable);
        }
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        gn {
            control {
                dscp-code-point value;
                echo-interval interval;
                echo-n3-requests requests;
                echo-t3-response response-interval;
                forwarding-class class-name;
                interface {
                    interface-name;
                    v4-address v4-address;
                }
                n3-requests requests;
                path-management (disable | enable);
                t3-response response-interval;
            }
            data {
                echo-interval interval;
                echo-n3-requests requests;
                echo-t3-response response-interval;
                interface {
                    interface-name;
```

```

        v4-address v4-address;
    }
    n3-requests requests;
    path-management (disable | enable);
    t3-response response-interval;
}
echo-interval interval;
echo-n3-requests requests;
echo-t3-response response-interval;
interface {
    interface-name;
    v4-address v4-address;
}
n3-requests requests;
path-management (disable | enable);
t3-response response-interval;
}
gp {
    control {
        dscp-code-point value;
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        forwarding-class class-name;
        interface {
            interface-name;
            v4-address v4-address;
        }
        n3-requests requests;
        path-management (disable | enable);
        t3-response response-interval;
    }
    data {
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        interface {
            interface-name;
            v4-address v4-address;
        }
        n3-requests requests;
        path-management (disable | enable);
        t3-response response-interval;
    }
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    interface {
        interface-name;
        v4-address v4-address;
    }
    n3-requests requests;
    path-management (disable | enable);
    t3-response response-interval;
}
interface {

```

```
    interface-name;
    v4-address v4-address;
}
n3-requests requests;
path-management (disable | enable);
peer-group name {
    control {
        support-16-bit-sequence;
    }
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    n3-requests requests;
    path-management (disable | enable);
    peer {
        [ip-addr-prefix];
    }
    routing-instance routing-identifier;
    t3-response response-interval;
}
peer-history number;
s5 {
    control {
        dscp-code-point value;
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        forwarding-class class-name;
        interface {
            interface-name;
            v4-address v4-address;
        }
        n3-requests requests;
        path-management (disable | enable);
        support-16-bit-sequence;
        t3-response response-interval;
    }
    data {
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        interface {
            interface-name;
            v4-address v4-address;
        }
        n3-requests requests;
        path-management (disable | enable);
        t3-response response-interval;
    }
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    interface {
        interface-name;
        v4-address v4-address;
    }
}
```



```

n3-requests requests;
path-management (disable | enable);
t3-response response-interval;
}
s8 {
control {
dscp-code-point value;
echo-interval interval;
echo-n3-requests requests;
echo-t3-response response-interval;
forwarding-class class-name;
interface {
interface-name;
v4-address v4-address;
}
n3-requests requests;
path-management (disable | enable);
support-16-bit-sequence;
t3-response response-interval;
}
data {
echo-interval interval;
echo-n3-requests requests;
echo-t3-response response-interval;
interface {
interface-name;
v4-address v4-address;
}
n3-requests requests;
path-management (disable | enable);
t3-response response-interval;
}
echo-interval interval;
echo-n3-requests requests;
echo-t3-response response-interval;
interface {
interface-name;
v4-address v4-address;
}
n3-requests requests;
path-management (disable | enable);
t3-response response-interval;
}
t3-response response-interval;
traceoptions {
file filename {
files files;
(no-world-readable | world-readable);
size size;
}
flag {
flag;
}
level level;
no-remote-trace;
}

```

```
}
```

Hierarchy Level [edit unified-edge gateways ggsn-pgw]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the parameters related to the GPRS tunneling protocol (GTP) on the Gateway GPRS Support Node (GGSN) or Packet Data Network Gateway (P-GW). GTP is used to tunnel GTP packets through 3G and 4G networks. 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. A MobileNext Broadband Gateway configured as a GGSN, 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.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation • [Configuring GTP Services Overview on page 226](#)

gtp (S-GW)

```
Syntax  gtp {
    control {
        ddn-delay-sync (disable | enable);
        dscp-code-point value;
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        forwarding-class class-name;
        interface {
            interface-name;
            v4-address v4-address;
        }
        n3-requests requests;
        no-response-cache;
        path-management (disable | enable);
        response-cache-timeout t interval-in-seconds;
        t3-response response-interval;
        ttl-value ttl-value;
    }
    data {
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        error-indication-interval seconds;
        indirect-tunnel (disable | enable);
        interface {
            interface-name;
            v4-address v4-address;
        }
        num-gtpu-end-markers num-gtpu-end-markers;
        path-management (disable | enable);
    }
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    interface {
        interface-name;
        v4-address v4-address;
    }
    n3-requests requests;
    path-management (disable | enable);
    peer-history number;
    s11 {
        dscp-code-point value;
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        interface {
            interface-name;
            v4-address v4-address;
        }
        n3-requests requests;
    }
}
```

```
    path-management (disable | enable);
    t3-response response-interval;
    ttl-value ttl-value;
}
s12 {
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    interface {
        interface-name;
        v4-addressv4-address;
    }
    path-management (disable | enable);
}
s1u {
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    interface {
        interface-name;
        v4-addressv4-address;
    }
    path-management (disable | enable);
}
s4 {
    control {
        dscp-code-point value;
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        forwarding-class class-name;
        interface {
            interface-name;
            v4-addressv4-address;
        }
        n3-requests requests;
        path-management (disable | enable);
        t3-response response-interval;
        ttl-value ttl-value;
    }
    data {
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        interface {
            interface-name;
            v4-addressv4-address;
        }
        path-management (disable | enable);
    }
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    interface {
        interface-name;
        v4-addressv4-address;
```

```

    }
    n3-requests requests;
    path-management (disable | enable);
    t3-response response-interval;
  }
s5 {
  control {
    dscp-code-point value;
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    forwarding-class class-name;
    interface {
      interface-name;
      v4-address v4-address;
    }
    n3-requests requests;
    path-management (disable | enable);
    t3-response response-interval;
    ttl-value ttl-value;
  }
  data {
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    interface {
      interface-name;
      v4-address v4-address;
    }
    path-management (disable | enable);
  }
  echo-interval interval;
  echo-n3-requests requests;
  echo-t3-response response-interval;
  interface {
    interface-name;
    v4-address v4-address;
  }
  n3-requests requests;
  path-management (disable | enable);
  t3-response response-interval;
}
s8 {
  control {
    dscp-code-point value;
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    forwarding-class class-name;
    interface {
      interface-name;
      v4-address v4-address;
    }
    n3-requests requests;
    path-management (disable | enable);
    t3-response response-interval;
  }

```

```

    ttl-value ttl-value;
  }
  data {
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    interface {
      interface-name;
      v4-address v4-address;
    }
    path-management (disable | enable);
  }
  echo-interval interval;
  echo-n3-requests requests;
  echo-t3-response response-interval;
  interface {
    interface-name;
    v4-address v4-address;
  }
  n3-requests requests;
  path-management (disable | enable);
  t3-response response-interval;
}
t3-response response-interval;
traceoptions {
  file filename {
    files files;
    (no-world-readable | world-readable);
    size size;
  }
  flag {
    flag;
  }
  level level;
  no-remote-trace;
}
}

```

Hierarchy Level [edit unified-edge gateways *sgw gateway-name*]

Release Information Statement introduced in Junos OS Mobility Release 11.4W.

Description Configure the parameters related to the GPRS tunneling protocol (GTP) on the Serving Gateway (S-GW). GTP is used to tunnel GTP packets through 3G and 4G networks. Only GTP Version 2 is supported on the S-GW.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring General GTP Service on the S-GW on page 249](#)

indirect-tunnel

Syntax	<code>indirect-tunnel (disable enable);</code>
Hierarchy Level	[edit unified-edge gateways <i>sgw gateway-name</i> gtp data]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	<p>Specify whether support for indirect tunnel forwarding should be disabled or enabled. Indirect tunnel forwarding is enabled by default.</p> <p>To ensure minimal packet loss, network elements must switch the packet forwarding path from source eNodeB to target eNodeB, or, in inter-RAT scenarios, between eNodeB to Serving GPRS Support Node (SGSN) or Radio Network Controller (RNC), or SGSN to eNodeB.</p> <p>If a direct path is available, then the packets are routed directly between the network elements. If a direct path between the network elements is not available, then the packets are routed indirectly from the source eNodeB, RNC, or SGSN to the target eNodeB, RNC, or SGSN via the Serving Gateway (S-GW), or the source and target S-GWs (in the case of S-GW relocation). Indirect tunnels might be set up in the S-GW that is not hosting subscriber sessions.</p>
Options	<p>disable—Disable support for indirect tunnel forwarding.</p> <p>enable—Enable support for indirect tunnel forwarding.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring General GTP Service on the S-GW on page 249 • gtp (S-GW) on page 941

interface (GTP)

Syntax interface {
 interface-name;
 v4-address *v4-address*;
 }

Hierarchy Level [edit unified-edge gateways *ggsn-pgw name* gtp],
 [edit unified-edge gateways *ggsn-pgw name* gtp control],
 [edit unified-edge gateways *ggsn-pgw name* gtp data],
 [edit unified-edge gateways *ggsn-pgw name* gtp gn],
 [edit unified-edge gateways *ggsn-pgw name* gtp gn control],
 [edit unified-edge gateways *ggsn-pgw name* gtp gn data],
 [edit unified-edge gateways *ggsn-pgw name* gtp gp],
 [edit unified-edge gateways *ggsn-pgw name* gtp gp control],
 [edit unified-edge gateways *ggsn-pgw name* gtp gp data],
 [edit unified-edge gateways *ggsn-pgw name* gtp s5],
 [edit unified-edge gateways *ggsn-pgw name* gtp s5 control],
 [edit unified-edge gateways *ggsn-pgw name* gtp s5 data],
 [edit unified-edge gateways *ggsn-pgw name* gtp s8],
 [edit unified-edge gateways *ggsn-pgw name* gtp s8 control],
 [edit unified-edge gateways *ggsn-pgw name* gtp s8 data],
 [edit unified-edge gateways *sgw name* gtp],
 [edit unified-edge gateways *sgw name* gtp control],
 [edit unified-edge gateways *sgw name* gtp data],
 [edit unified-edge gateways *sgw name* gtp s11],
 [edit unified-edge gateways *sgw name* gtp s12],
 [edit unified-edge gateways *sgw name* gtp s1u],
 [edit unified-edge gateways *sgw name* gtp s4],
 [edit unified-edge gateways *sgw name* gtp s4 control],
 [edit unified-edge gateways *sgw name* gtp s4 data],
 [edit unified-edge gateways *sgw name* gtp s5],
 [edit unified-edge gateways *sgw name* gtp s5 control],
 [edit unified-edge gateways *sgw name* gtp s5 data],
 [edit unified-edge gateways *sgw name* gtp s8],
 [edit unified-edge gateways *sgw name* gtp s8 control],
 [edit unified-edge gateways *sgw name* gtp s8 data]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.
 Support at the following hierarchy levels introduced in Junos OS Mobility Release 11.4W:

- [edit unified-edge gateways *sgw name* gtp]
- [edit unified-edge gateways *sgw name* gtp control]
- [edit unified-edge gateways *sgw name* gtp data]
- [edit unified-edge gateways *sgw name* gtp s11]
- [edit unified-edge gateways *sgw name* gtp s12]
- [edit unified-edge gateways *sgw name* gtp s1u]
- [edit unified-edge gateways *sgw name* gtp s4]
- [edit unified-edge gateways *sgw name* gtp s4 control]

- [edit unified-edge gateways *sgw name* gtp s4 data]
- [edit unified-edge gateways *sgw name* gtp s5]
- [edit unified-edge gateways *sgw name* gtp s5 control]
- [edit unified-edge gateways *sgw name* gtp s5 data]
- [edit unified-edge gateways *sgw name* gtp s8]
- [edit unified-edge gateways *sgw name* gtp s8 control]
- [edit unified-edge gateways *sgw name* gtp s8 data]

Description Specify the loopback interface and IPv4 address on which the GTP packets are received. To enable GTP services, you must configure at least one loopback interface and IPv4 address for the Gateway GPRS Support Node (GGSN) or Packet Data Network Gateway (P-GW) or for the Serving Gateway (S-GW), as applicable.

For the GGSN or P-GW, you can optionally configure the loopback interface and IP address at the Gn, Gp, S5, or S8 interface levels or their corresponding control and data planes, or at the gateway level or their corresponding control and data planes.

For the S-GW, you can optionally configure the loopback interface and IP address at the S11, S12, or S1u interface levels, or the S4, S5, or S8 interface levels, or their corresponding control and data planes, or at the gateway level or their corresponding control and data planes. However, you must at least configure the **interface** statement:

- At the [edit unified-edge gateways *sgw name* gtp] hierarchy level or the [edit unified-edge gateways *sgw name* gtp control] and [edit unified-edge gateways *sgw name* gtp data] hierarchy levels, or
- If it is not configured at the top of the GTP hierarchy level, you must configure the statement for either:
 - The S11, S1u, and one of the S5 or S8 interfaces, or
 - The S4, and one of the S5 or S8 interfaces.

Options *interface-name*—Name of the interface used in the gateway.

v4-address v4-address—IP address (IPv4) on which the GTP packets are received.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring GTP Services Overview on page 226](#)
- [gtp \(GGSN or P-GW\) on page 936](#)
- [gtp \(S-GW\) on page 941](#)

n3-requests

Syntax	<code>n3-requests <i>requests</i>;</code>
Hierarchy Level	<code>[edit unified-edge gateways ggsn-pgw <i>name</i> gtp],</code> <code>[edit unified-edge gateways ggsn-pgw <i>name</i> gtp control],</code> <code>[edit unified-edge gateways ggsn-pgw <i>name</i> gtp gn],</code> <code>[edit unified-edge gateways ggsn-pgw <i>name</i> gtp gn control],</code> <code>[edit unified-edge gateways ggsn-pgw <i>name</i> gtp gn data],</code> <code>[edit unified-edge gateways ggsn-pgw <i>name</i> gtp gp],</code> <code>[edit unified-edge gateways ggsn-pgw <i>name</i> gtp gp control],</code> <code>[edit unified-edge gateways ggsn-pgw <i>name</i> gtp gp data],</code> <code>[edit unified-edge gateways ggsn-pgw <i>name</i> gtp peer-group <i>name</i>],</code> <code>[edit unified-edge gateways ggsn-pgw <i>name</i> gtp s5],</code> <code>[edit unified-edge gateways ggsn-pgw <i>name</i> gtp s5 control],</code> <code>[edit unified-edge gateways ggsn-pgw <i>name</i> gtp s5 data],</code> <code>[edit unified-edge gateways ggsn-pgw <i>name</i> gtp s8],</code> <code>[edit unified-edge gateways ggsn-pgw <i>name</i> gtp s8 control],</code> <code>[edit unified-edge gateways ggsn-pgw <i>name</i> gtp s8 data],</code> <code>[edit unified-edge gateways sgw <i>name</i> gtp],</code> <code>[edit unified-edge gateways sgw <i>name</i> gtp control],</code> <code>[edit unified-edge gateways sgw <i>name</i> gtp s11],</code> <code>[edit unified-edge gateways sgw <i>name</i> gtp s4],</code> <code>[edit unified-edge gateways sgw <i>name</i> gtp s4 control],</code> <code>[edit unified-edge gateways ggsn-pgw <i>name</i> gtp s5],</code> <code>[edit unified-edge gateways ggsn-pgw <i>name</i> gtp s5 control],</code> <code>[edit unified-edge gateways ggsn-pgw <i>name</i> gtp s8],</code> <code>[edit unified-edge gateways ggsn-pgw <i>name</i> gtp s8 control],</code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the following hierarchy levels introduced in Junos OS Mobility Release 11.4W: <ul style="list-style-type: none">• <code>[edit unified-edge gateways sgw <i>name</i> gtp]</code>• <code>[edit unified-edge gateways sgw <i>name</i> gtp control]</code>• <code>[edit unified-edge gateways sgw <i>name</i> gtp s11]</code>• <code>[edit unified-edge gateways sgw <i>name</i> gtp s4]</code>• <code>[edit unified-edge gateways sgw <i>name</i> gtp s4 control]</code>• <code>[edit unified-edge gateways sgw <i>name</i> gtp s5]</code>• <code>[edit unified-edge gateways sgw <i>name</i> gtp s5 control]</code>• <code>[edit unified-edge gateways sgw <i>name</i> gtp s8]</code>• <code>[edit unified-edge gateways sgw <i>name</i> gtp s8 control]</code>
Description	For tunnel management, configure the maximum number of times that the broadband gateway attempts to send a signaling request message to a control. The gateway waits for the time specified in the <code>t3-timeout</code> statement before resending a signaling request message when a response to the request has not been received.

Options	<p>requests—Maximum number of times that the gateway attempts to send a signaling request message.</p> <p>Range: 1 through 5</p> <p>Default: 3</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring GTP Services Overview on page 226 • gtp (GGSN or P-GW) on page 936 • gtp (S-GW) on page 941

no-response-cache

Syntax	no-response-cache;
Hierarchy Level	<p>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> gtp control],</p> <p>[edit unified-edge gateways sgw <i>gateway-name</i> gtp control]</p>
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	<p>Specify that the GPRS Tunneling Protocol (GTP) response cache is disabled. The response cache stores the GTP responses (sent for request messages) for the duration configured, or the default, if the time is not configured, using the response-cache-timeout statement. If this cache is disabled, then the response messages are not stored.</p>
Default	If you do not configure this statement, then the GTP response cache is enabled by default.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring General GTP Service on the S-GW on page 249 • gtp (GGSN or P-GW) on page 936 • gtp (S-GW) on page 941 • response-cache-timeout on page 955

num-gtpu-end-markers

Syntax	<code>num-gtpu-end-markers <i>num-gtpu-end-markers</i>;</code>
Hierarchy Level	[edit unified-edge gateways <i>sgw gateway-name</i> gtp data]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Configure the number of GPRS tunneling protocol, user plane (GTP-U) end marker packets to be sent in case of handovers towards the previous access tunnel for the bearer.
Options	<p><i>num-gtpu-end-markers</i>—Number of GTP-U end marker packets.</p> <p>Range: 0 through 10, where 0 indicates that the sending of GTP-U end marker packets is disabled.</p> <p>Default: 1</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring General GTP Service on the S-GW on page 249• gtp (S-GW) on page 941

path-management

Syntax	<code>path-management (disable enable);</code>
Hierarchy Level	<pre> [edit unified-edge gateways ggsn-pgw <i>name</i> gtp], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp control], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp data], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp gn], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp gn control], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp gn data], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp gp], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp gp control], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp gp data], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp peer-group <i>name</i>], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s5], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s5 control], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s5 data], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s8], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s8 control], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s8 data], [edit unified-edge gateways sgw <i>name</i> gtp], [edit unified-edge gateways sgw <i>name</i> gtp control], [edit unified-edge gateways sgw <i>name</i> gtp data], [edit unified-edge gateways sgw <i>name</i> gtp s11], [edit unified-edge gateways sgw <i>name</i> gtp s12], [edit unified-edge gateways sgw <i>name</i> gtp s1u], [edit unified-edge gateways sgw <i>name</i> gtp s4], [edit unified-edge gateways sgw <i>name</i> gtp s4 control], [edit unified-edge gateways sgw <i>name</i> gtp s4 data], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s5], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s5 control], [edit unified-edge gateways sgw <i>name</i> gtp s5 data], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s8], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s8 control], [edit unified-edge gateways sgw <i>name</i> gtp s8 data] </pre>
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W.</p> <p>Support at the following hierarchy levels introduced in Junos OS Mobility Release 11.4W:</p> <ul style="list-style-type: none"> • <code>[edit unified-edge gateways sgw <i>name</i> gtp]</code> • <code>[edit unified-edge gateways sgw <i>name</i> gtp control]</code> • <code>[edit unified-edge gateways sgw <i>name</i> gtp data]</code> • <code>[edit unified-edge gateways sgw <i>name</i> gtp s11]</code> • <code>[edit unified-edge gateways sgw <i>name</i> gtp s12]</code> • <code>[edit unified-edge gateways sgw <i>name</i> gtp s1u]</code> • <code>[edit unified-edge gateways sgw <i>name</i> gtp s4]</code> • <code>[edit unified-edge gateways sgw <i>name</i> gtp s4 control]</code> • <code>[edit unified-edge gateways sgw <i>name</i> gtp s4 data]</code>

- [edit unified-edge gateways *sgw name* gtp s5]
- [edit unified-edge gateways *sgw name* gtp s5 control]
- [edit unified-edge gateways *sgw name* gtp s5 data]
- [edit unified-edge gateways *sgw name* gtp s8]
- [edit unified-edge gateways *sgw name* gtp s8 control]
- [edit unified-edge gateways *sgw name* gtp s8 data]

Description	Enable or disable path management. When path management is disabled, the broadband gateway does not send echo request messages to its peer. By default, path management is enabled only on the control plane for the broadband gateway.
Options	disable —Disable path management. enable —Enable path management.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring GTP Services Overview on page 226• gtp (GGSN or P-GW) on page 936• gtp (S-GW) on page 941

peer (GTP)

Syntax	<pre>peer { [<i>ip-addr-prefix</i>]; }</pre>
Hierarchy Level	[edit unified-edge gateways <i>ggsn-pgw name</i> gtp peer-group <i>peer-group</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the IP address of the peer in the peer group. The IP address specified must also include the network prefix. To specify multiple peers, include the peer statement multiple times.
Options	ip-addr-prefix —IP address of the peer, including the network prefix; for example, 22.1.1.10/16.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring GTP Services Overview on page 226• peer-group (GTP) on page 953


peer-group (GTP)

Syntax	<pre>peer-group <i>name</i> { control { support-16-bit-sequence; } echo-interval <i>interval</i>; echo-n3-requests <i>requests</i>; echo-t3-response <i>response-interval</i>; n3-requests <i>requests</i>; path-management (disable enable); peer { [<i>ip-addr-prefix</i>]; } routing-instance <i>routing-identifier</i>; t3-response <i>response-interval</i>; }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>name</i> gtp]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure a group of 3GPP GTP peers to share common signaling and data parameters. This configuration overrides the common or interface-specific configuration for the peers in the group.
Options	<p><i>name</i>—Name of the peer group.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring GTP Services Overview on page 226 • gtp (GGSN or P-GW) on page 936 • gtp (S-GW) on page 941

peer-history (GTP)

Syntax	<code>peer-history <i>number</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>name</i> gtp], [edit unified-edge gateways sgw <i>name</i> gtp]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>name</i> gtp] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Configure the maximum number of peers (that are no longer present on the broadband gateway) for which the broadband gateway stores the statistics collected.
Options	<i>number</i> —Maximum number of peers for which statistics are stored. Range: 1 through 1000
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring GTP Services Overview on page 226• gtp (GGSN or P-GW) on page 936• gtp (S-GW) on page 941

response-cache-timeout

Syntax	<code>response-cache-timeout <i>interval-in-seconds</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> gtp control], [edit unified-edge gateways sgw <i>gateway-name</i> gtp control]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Configure the timeout for the GPRS Tunneling Protocol (GTP) response cache. This timeout indicates the duration for which the GTP response messages (sent for request messages) should be stored in the response cache.
<div>  <p>NOTE: This configuration is invalid if the <code>no-response-cache</code> statement is configured.</p> </div>	
Options	<p><i>timeout-in-seconds</i>—Timeout, in seconds, for the GTP response cache.</p> <p>Range: 5 through 20 seconds</p> <p>Default: 15 seconds</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring General GTP Service on the S-GW on page 249 • gtp (GGSN or P-GW) on page 936 • gtp (S-GW) on page 941 • no-response-cache on page 949

routing-instance (GTP)

Syntax	<code>routing-instance <i>routing-identifier</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>name</i> gtp peer-group <i>name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the routing instance or the VPN routing and forwarding (VRF) instance for the peer group.
Options	<i>routing-identifier</i> —Identifier for the routing instance.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring GTP Services Overview on page 226• peer-group (GTP) on page 953

s11

Syntax

```
s11 {
  dscp-code-point value;
  echo-interval interval;
  echo-n3-requests requests;
  echo-t3-response response-interval;
  interface {
    interface-name;
    v4-address v4-address;
  }
  n3-requests requests;
  path-management (disable | enable);
  t3-response response-interval;
  ttl-value ttl-value;
}
```

Hierarchy Level [edit unified-edge gateways *sgw gateway-name* gtp]

Release Information Statement introduced in Junos OS Mobility Release 11.4W.

Description Configure the 3GPP control and data parameters applicable to the 3GPP s11 interface. The s11 interface is used by the serving gateway and the Mobile Management Entity (MME) to exchange GTP-C control packets with each other.

The values configured here override the common control and data configuration configured at the [edit unified-edge gateways *sgw gateway-name* gtp] hierarchy level. The parameters configured here are applicable to all GTP peers that use the interface.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring GTP-C Services on the S11 Interface on page 252](#)
- [gtp \(S-GW\) on page 941](#)

s12

Syntax	<pre>s12 { echo-interval <i>interval</i>; echo-n3-requests <i>requests</i>; echo-t3-response <i>response-interval</i>; interface { interface-name; v4-address <i>v4-address</i>; } path-management (disable enable); }</pre>
Hierarchy Level	[edit unified-edge gateways <i>sgw gateway-name</i> gtp]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the 3GPP data parameters applicable to the 3GPP s12 interface. The s12 interface is used by the serving gateway and the Radio Network Controller (RNC) to exchange GTP user plane (GTP-U) data packets with each other.</p> <p>The values configured here override the common data configuration configured at the [edit unified-edge gateways <i>sgw gateway-name</i> gtp] hierarchy level. The parameters configured here are applicable to all GTP peers that use the interface.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring GTP-U Services on the S12 Interface on page 254• gtp (S-GW) on page 941

s1u

Syntax	<pre>s1u { echo-interval <i>interval</i>; echo-n3-requests <i>requests</i>; echo-t3-response <i>response-interval</i>; interface { <i>interface-name</i>; v4-address <i>v4-address</i>; } path-management (disable enable); }</pre>
Hierarchy Level	[edit unified-edge gateways sgw <i>gateway-name</i> gtp]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the 3GPP data parameters applicable to the 3GPP s1u interface. The s1u interface is used by the serving gateway and the eNodeB to exchange GTP user plane (GTP-U) data packets with each other.</p> <p>The values configured here override the common data configuration configured at the [edit unified-edge gateways sgw <i>gateway-name</i> gtp] hierarchy level. The parameters configured here are applicable to all GTP peers that use the interface.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring GTP Services on the S1-U Interface on page 256 • gtp (S-GW) on page 941

s4

```

Syntax  s4 {
        control {
            dscp-code-point value;
            echo-interval interval;
            echo-n3-requests requests;
            echo-t3-response response-interval;
            forwarding-class class-name;
            interface {
                interface-name;
                v4-address v4-address;
            }
            n3-requests requests;
            path-management (disable | enable);
            t3-response response-interval;
            ttl-value ttl-value;
        }
        data {
            echo-interval interval;
            echo-n3-requests requests;
            echo-t3-response response-interval;
            forwarding-class class-name;
            interface {
                interface-name;
                v4-address v4-address;
            }
            path-management (disable | enable);
        }
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        interface {
            interface-name;
            v4-address v4-address;
        }
        n3-requests requests;
        path-management (disable | enable);
        t3-response response-interval;
    }

```

Hierarchy Level [edit unified-edge gateways *sgw gateway-name* gtp]

Release Information Statement introduced in Junos OS Mobility Release 11.4W.

Description Configure the 3GPP control and data parameters applicable to the 3GPP S4 interface. The S4 interface is used by the serving gateway and the S4 Serving GPRS Support Nodes (SGSNs).

The values configured here override the common control and data configuration configured at the [edit unified-edge gateways *sgw gateway-name* gtp] hierarchy level. The parameters configured here are applicable to all GTP peers that use the interface.

The remaining statements are explained separately.

Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring GTP Services on the S4 Interface on page 257• gtp (S-GW) on page 941

s5

```

Syntax  s5 {
        control {
            dscp-code-point value;
            echo-interval interval;
            echo-n3-requests requests;
            echo-t3-response response-interval;
            forwarding-class class-name;
            interface {
                interface-name;
                v4-address v4-address;
            }
            n3-requests requests;
            path-management (disable | enable);
            support-16-bit-sequence; #P-GW only
            t3-response response-interval;
            ttl-value ttl-value; #S-GW only
        }
        data {
            echo-interval interval;
            echo-n3-requests requests;
            echo-t3-response response-interval;
            interface {
                interface-name;
                v4-address v4-address;
            }
            n3-requests requests; #P-GW only
            path-management (disable | enable);
            t3-response response-interval; #P-GW only
        }
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        interface {
            interface-name;
            v4-address v4-address;
        }
        n3-requests requests;
        path-management (disable | enable);
        t3-response response-interval;
    }

```

Hierarchy Level [edit unified-edge gateways *ggsn-pgw name gtp*],
[edit unified-edge gateways *sgw name gtp*],

Release Information Statement introduced in Junos OS Mobility Release 11.2W.
Support at the [edit unified-edge gateways *sgw name gtp*] hierarchy level introduced in Junos OS Mobility Release 11.4W.

Description Configure the path and tunnel management parameters for the 3GPP S5 interface. This configuration overrides the parameters configured at a higher level in the hierarchy and applies to all GTP peers that connect to the S5 interface. You can also configure

parameters only for GTP control packets or GTP user plane packets—these parameters override the parameters at the higher hierarchy levels.

The remaining statements are explained separately.

Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring GTP Services Overview on page 226• gtp (GGSN or P-GW) on page 936• gtp (S-GW) on page 941

s8

```

Syntax  s8 {
        control {
            dscp-code-point value;
            echo-interval interval;
            echo-n3-requests requests;
            echo-t3-response response-interval;
            forwarding-class class-name;
            interface {
                interface-name;
                v4-address v4-address;
            }
            n3-requests requests;
            path-management (disable | enable);
            support-16-bit-sequence; #P-GW only
            t3-response response-interval;
            ttl-value ttl-value; #S-GW only
        }
        data {
            echo-interval interval;
            echo-n3-requests requests;
            echo-t3-response response-interval;
            interface {
                interface-name;
                v4-address v4-address;
            }
            n3-requests requests; #P-GW only
            path-management (disable | enable);
            t3-response response-interval; #P-GW only
        }
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        interface {
            interface-name;
            v4-address v4-address;
        }
        n3-requests requests;
        path-management (disable | enable);
        t3-response response-interval;
    }

```

Hierarchy Level [edit unified-edge gateways *ggsn-pgw name gtp*],
[edit unified-edge gateways *sgw name gtp*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.
Support at the [edit unified-edge gateways *sgw name gtp*] hierarchy level introduced in Junos OS Mobility Release 11.4W.

Description Configure the path and tunnel management parameters for the 3GPP S8 interface. This configuration overrides the parameters configured at a higher level in the hierarchy and applies to all GTP peers that connect to the S8 interface. You can also configure

parameters only for GTP control packets or GTP user plane packets—these parameters override the parameters at the higher hierarchy levels.

The remaining statements are explained separately.

Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring GTP Services Overview on page 226 • gtp (GGSN or P-GW) on page 936 • gtp (S-GW) on page 941

support-16-bit-sequence

Syntax	support-16-bit-sequence;
Hierarchy Level	[edit unified-edge gateways ggsn-pgw name gtp peer-group name control], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s5 control], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s8 control]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Enable support for 16-bit sequence numbers for interoperation with older gateways that support a GTP version with a 16-bit sequence number length. Support for 16-bit sequence numbers is disabled by default.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring GTP Services Overview on page 226 • gtp (GGSN or P-GW) on page 936 • gtp (S-GW) on page 941

t3-response

Syntax	<code>t3 response <i>response-interval</i>;</code>
Hierarchy Level	<pre> [edit unified-edge gateways ggsn-pgw <i>name</i> gtp], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp control], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp gn], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp gn control], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp gn data], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp gp], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp gp control], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp gp data], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp peer-group <i>name</i>], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s5], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s5 control], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s5 data], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s8], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s8 control], [edit unified-edge gateways ggsn-pgw <i>name</i> gtp s8 data], [edit unified-edge gateways sgw <i>name</i> gtp], [edit unified-edge gateways sgw <i>name</i> gtp control], [edit unified-edge gateways sgw <i>name</i> gtp s11], [edit unified-edge gateways sgw <i>name</i> gtp s4], [edit unified-edge gateways sgw <i>name</i> gtp s4 control], [edit unified-edge gateways sgw <i>name</i> gtp s5], [edit unified-edge gateways sgw <i>name</i> gtp s5 control], [edit unified-edge gateways sgw <i>name</i> gtp s8], [edit unified-edge gateways sgw <i>name</i> gtp s8 control] </pre>
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W.</p> <p>Support at the following hierarchy levels introduced in Junos OS Mobility Release 11.4W:</p> <ul style="list-style-type: none"> • <code>[edit unified-edge gateways sgw <i>name</i> gtp]</code> • <code>[edit unified-edge gateways sgw <i>name</i> gtp control]</code> • <code>[edit unified-edge gateways sgw <i>name</i> gtp s11]</code> • <code>[edit unified-edge gateways sgw <i>name</i> gtp s4]</code> • <code>[edit unified-edge gateways sgw <i>name</i> gtp s4 control]</code> • <code>[edit unified-edge gateways sgw <i>name</i> gtp s5]</code> • <code>[edit unified-edge gateways sgw <i>name</i> gtp s5 control]</code> • <code>[edit unified-edge gateways sgw <i>name</i> gtp s8]</code> • <code>[edit unified-edge gateways sgw <i>name</i> gtp s8 control]</code>
Description	Configure the response timeout for GTP signaling request messages. The response timeout is how long the gateway waits before resending a signaling request message when the response to a request has not been received.
Options	<i>seconds</i> —Time that the gateway waits before resending a signaling request message.

Range: 1 through 30 seconds

Default: 5 seconds

Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring GTP Services Overview on page 226• gtp (GGSN or P-GW) on page 936• gtp (S-GW) on page 941

traceoptions (GTP)

Syntax	<pre>traceoptions { file <i>filename</i> { files <i>files</i>; (no-world-readable world-readable); size <i>size</i>; } flag { <i>flag</i>; } level <i>level</i>; no-remote-trace; }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>name</i> gtp], [edit unified-edge gateways sgw <i>name</i> gtp]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>name</i> gtp] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Configure GTP tracing options. You can specify which trace operations are logged by including specific tracing flags and levels.
Options	<p>file <i>filename</i>—Name of the file that receives the output of the tracing operation. All files are placed in the <code>/var/log</code> directory.</p> <p>files <i>files</i>— (Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you must also specify a maximum file size with the size option and a filename.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag</p> <ul style="list-style-type: none">• flag—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can use one of the following flags:<ul style="list-style-type: none">• all—Trace everything.• config—Trace configuration-related information.• debug—Trace debug information.• decode—Trace decoding of received packets.• encode—Trace encoding of transmitted packets.

- **error**—Trace internal and external errors.
- **events**—Trace all internal and external events.
- **packet-io**—Trace transmitted and received packets.
- **peer**—Trace GTP peer-related events.
- **tracker**—Trace GTP tracker-related events.
- **warning**—Trace warnings.

level *level*—(Optional) Level of tracing to perform. You can specify any of the following levels:

- **all**—Match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match conditions that should be handled specially
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

no-remote-trace—(Optional) Disable remote tracing.

no-world-readable—(Optional) Restrict access to the originator of the trace operation only.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you must also specify a maximum number of trace files with the **files** option and filename.

Syntax: **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring GTP Services Overview on page 226](#)
- [gtp \(GGSN or P-GW\) on page 936](#)
- [gtp \(S-GW\) on page 941](#)

ttl-value (S-GW GTP-C)

Syntax	<code>ttl-value <i>ttl-value</i>;</code>
Hierarchy Level	[edit unified-edge gateways sgw <i>gateway-name</i> gtp control], [edit unified-edge gateways sgw <i>gateway-name</i> gtp s4 control], [edit unified-edge gateways sgw <i>gateway-name</i> gtp s5 control], [edit unified-edge gateways sgw <i>gateway-name</i> gtp s8 control], [edit unified-edge gateways sgw <i>gateway-name</i> gtp s11]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Configure the time-to-live (TTL) value used on outgoing GPRS tunneling protocol, control plane (GTP-C) packets. When the TTL count in the GTP-C packet reaches zero, the packet is discarded.
Options	ttl-value —TTL value Range: 1 through 255 Default: 255
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring General GTP Service on the S-GW on page 249• control (GTP) on page 917

Service Applications Configuration Statements

egress-key (Aggregated Multiservices)

Syntax	<code>egress-key (destination-ip source-ip);</code>
Hierarchy Level	[edit services service-set <i>service-set-name</i> interface-service load-balancing-options hash-keys]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the hash keys to be used in the egress flow direction. The configuration is mandatory if you are using AMS for Network Address Translation (NAT). This configuration is not mandatory if you are using AMS for stateful firewall; if the hash keys are not configured, then the defaults are chosen. (See hash-keys (Aggregated Multiservices) for more information.)
Options	<p>The following hash keys can be configured in the egress direction:</p> <p>destination-ip—Use the destination IP address of the flow to compute the hash used in load balancing.</p> <p>source-ip—Use the source IP address of the flow to compute the hash used in load balancing.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • hash-keys (Aggregated Multiservices) on page 972

hash-keys (Aggregated Multiservices)

Syntax	<pre>hash-keys { egress-key (destination-ip source-ip); ingress-key (destination-ip source-ip); resource-triggered; }</pre>
Hierarchy Level	[edit services service-set <i>service-set-name</i> interface-service load-balancing-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the hash keys used for load balancing in aggregated multiservices (AMS) for service applications (Network Address Translation [NAT], stateful firewall, application-level gateway [ALG], HTTP header enrichment, and mobility). The hash keys supported in the ingress and egress direction are the source IP address and destination IP address.</p> <p>Hash keys are used to define the load-balancing behavior among the various members in the AMS group. For example, if hash-keys is configured as source-ip, then the hashing would be performed based on the source IP address of the packet. Therefore, all packets with the same source IP address land on the same member. Hash keys must be configured with respect to the traffic direction: ingress or egress. For example, if hash-keys is configured as source-ip in the ingress direction, then it should be configured as destination-ip in the egress direction. This is required to ensure that the packets of the same flow reach the same member of the AMS group.</p> <p>The configuration of the ingress and egress hash keys is mandatory if you are using AMS for NAT. This configuration is not mandatory if you are using AMS for stateful firewall; if the hash keys are not configured, then the defaults are chosen. Refer to Table 56 on page 973 for the supported hash keys.</p> <p>The resource-triggered option enables anchor session PICs to use the load or resource information from the anchor services PICs to select the AMS member will anchor the services for the subscriber for load balancing among AMS members. In addition, for mobile subscriber-aware services (such as HTTP header enrichment), you must configure the resource-triggered statement, which means that the load balancing is not done using the ingress and egress keys.</p>

Table 56: Hash Keys Supported for AMS for Service Applications

Service Set at Ingress Interface			Service Set at Egress Interface	
Hash Keys for NAT				
NAT Type	Ingress hash key	Egress hash key	Ingress hash key	Egress hash key
source static	Destination IP address	Source IP address	Source IP address	Destination IP address
source dynamic	Source IP address	Destination IP address	Destination IP address	Source IP address
Network Address Port Translation (NAPT)	Source IP address	Destination IP address	Destination IP address	Source IP address
destination static	Source IP address	Destination IP address	Destination IP address	Source IP address
Hash Keys for Stateful Firewall				
Stateful Firewall	Destination IP address	Source IP address	Destination IP address	Source IP address
Stateful Firewall	Source IP address	Destination IP address	Source IP address	Destination IP address



NOTE: If NAT is used in the service set (along with stateful firewall and ALG), then the hash keys should be based on the NAT type; otherwise, the hash keys of the stateful firewall should be used.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation • [load-balancing-options \(Aggregated Multiservices for Services Applications\) on page 976](#)

ingress-key (Aggregated Multiservices)

Syntax	ingress-key (destination-ip source-ip);
Hierarchy Level	[edit services service-set <i>service-set-name</i> interface-service load-balancing-options hash-keys]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the hash keys to be used in the ingress flow direction. The configuration is mandatory if you are using AMS for Network Address Translation (NAT). This configuration is not mandatory if you are using AMS for stateful firewall; if the hash keys are not configured, then the defaults are chosen.
Options	<p>The following hash keys can be configured in the ingress direction:</p> <p>destination-ip—Use the destination IP address of the flow to compute the hash used in load balancing.</p> <p>source-ip—Use the source IP address of the flow to compute the hash used in load balancing.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• hash-keys (Aggregated Multiservices) on page 972

interface-service (Aggregated Multiservices)

Syntax

```
interface-service {
  load-balancing-options {
    hash-keys {
      egress-key (destination-ip | source-ip);
      ingress-key (destination-ip | source-ip);
      resource-triggered;
    }
  }
  service-interface interface-name.unit-number;
}
```

Hierarchy Level [edit services service-set *service-set-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Support for aggregated multiservices (AMS) interfaces introduced in Junos OS Mobility Release 11.2W.

Description Specify the interface name and unit number to be used in aggregated multiservices (AMS) with high availability (HA) for service applications (Network Address Translation [NAT], stateful firewall, application-level gateway [ALG], HTTP header enrichment, and mobility), and configure the load-balancing options in AMS with high availability for service applications.

Options **service-interface** *interface-name.unit-number*—Name and unit number of the AMS interface; for example, **ams0.1**, where **ams0** is the interface and **1** is the unit number.



NOTE: Unit 0 is reserved and cannot be configured under the AMS interface.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [service-set \(Aggregated Multiservices\) on page 978](#)

load-balancing-options (Aggregated Multiservices for Services Applications)

Syntax	<pre>load-balancing-options { hash-keys { egress-key (destination-ip source-ip); ingress-key (destination-ip source-ip); resource-triggered; } }</pre>
Hierarchy Level	[edit services service-set <i>service-set-name</i> interface-service]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the load-balancing options for aggregated multiservices (AMS) in service applications (Network Address Translation [NAT], stateful firewall, application-level gateway [ALG], HTTP header enrichment, and mobility). AMS for service applications can be used for load balancing with or without high availability (HA). Currently, load balancing is based on the configured hash keys.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• interface-service (Aggregated Multiservices) on page 975

resource-triggered (Aggregated Multiservices)

Syntax	resource-triggered;
Hierarchy Level	[edit services service-set <i>service-set-name</i> interface-service load-balancing-options hash-keys]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	<p>Specify that the load balancing for aggregated multiservices (AMS) for services applications should be triggered based on the resources (load) information from the services PICs.</p> <p>If the HTTP header enrichment service is configured as a mobility subscriber-aware service, then the anchor services PIC can be configured as either a multiservices interface (for example ms-1/0/0) or an AMS interface (for example ams0). If it is configured as an AMS interface, then the load balancing must be performed by the anchor session PICs, which are configured using the resource-triggered statement. Therefore, the resource-triggered statement is mandatory for subscriber-aware services using AMS interfaces.</p> <p>Only one service set can be configured with resource triggering as the load-balancing behavior.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • hash-keys (Aggregated Multiservices) on page 972

service-set (Aggregated Multiservices)

Syntax

```
service-set service-set-name {  
  interface-service {  
    load-balancing-options {  
      hash-keys {  
        egress-key (destination-ip | source-ip);  
        ingress-key (destination-ip | source-ip);  
        resource-triggered;  
      }  
    }  
    service-interface interface-name.unit-number;  
  }  
  [tag-rule-sets rule-set-name];  
  [tag-rules rule-name];  
  service-set-options {  
    subscriber-awareness;  
  }  
}
```

Hierarchy Level [edit services]

Release Information Statement introduced before Junos OS Release 7.4.
Support for aggregated multiservices (AMS) interfaces introduced in Junos OS Mobility Release 11.2W.

Description Configure the service set with aggregated multiservices (AMS) for load balancing in service applications. Currently, Network Address Translation (NAT), stateful firewall, application-level gateway (ALG), HTTP header enrichment, and mobility are the service applications supported.

The following ALGs are currently supported:

- FTP
- Internet Control Message Protocol (ICMP)
- Point-to-Point Tunneling Protocol (PPTP)
- Real-Time Streaming Protocol (RTSP)
- SQL *Net
- TCP
- traceroute
- Trivial File Transfer Protocol (TFTP)
- UDP

AMS for service applications (NAT, stateful firewall, and ALG) can be used for load balancing with or without high availability. Many-to-one (N:1) high availability (HA) is supported for service applications (NAT, stateful firewall, and ALG). In this case, one multiservices PIC is the backup for one or more (N) active multiservices PICs. If one of the active multiservices PICs goes down, then the backup replaces it as the active

multiservices PIC. When the failed PIC comes back online, it becomes the new backup. This is called floating backup mode.



NOTE: In high availability for service applications, the configuration state is synchronized to the backup. However, the operational state of the active members is not synchronized to the backup. Therefore, in the case of failure, existing flows meant for the failed member are lost.

The following conditions are applicable if you use AMS for load balancing in service applications:

- All the member interfaces of the AMS interface must have the same packages configured for the respective service applications. For example, if **mams-5/0/0** is the active member and **mams-5/1/0** the backup, then both **mams-5/0/0** and **mams-5/1/0** must have the same packages.
 - For NAT, the member interfaces must have the **jservices-nat** package configured.
 - For stateful firewall, the member interfaces must have the **jservices-sfw** package configured.
 - For ALG, the member interfaces must have the **jservices-alg** package configured.
- The size of the object cache (**object-cache-size**) and the size of the policy database (**policy-db-size**) must be appropriately configured so that the memory requirements of the services application policy database are met.
- For anchor session PICs, currently, AMS member PICs operate only in 64-bit mode. Therefore the **boot-os embedded-junos64** configuration, at the **[edit chassis fpc slot-number pic pic-number adaptive-services service-package extension-provider]** hierarchy level, is mandatory for all member interfaces.

The remaining statements are explained separately.

Options **service-set-name**—Name of the service set.

Required Privilege interface—To view this statement in the configuration.
Level interface-control—To add this statement to the configuration.

CHAPTER 28

System Architecture and Gateway Traceoptions Configuration Statements


- [System Architecture Configuration Statements on page 981](#)
- [Gateway Traceoptions Configuration Statements on page 1000](#)

System Architecture Configuration Statements

call-rate-statistics

Syntax	<pre>call-rate-statistics { history <i>history</i>; interval <i>interval</i>; }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i>], [edit unified-edge gateways sgw <i>gateway-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i>] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the parameters related to the broadband gateway's call-rate statistics. You can specify the number of past intervals for which the call-rate statistics are stored, and the interval for which the call-rate statistics are calculated.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• [edit unified-edge gateways] Hierarchy Level on page 563• show unified-edge ggsn-pgw call-rate statistics on page 1277• show unified-edge sgw call-rate statistics on page 1282

disable (Idle Mode Buffering)

Syntax	disable;
Hierarchy Level	[edit unified-edge gateways sgw <i>gateway-name</i> idle-mode-buffering]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	<p>Disable idle mode buffering on the Serving Gateway (S-GW). When idle mode buffering is disabled, the S-GW does <i>not</i> buffer the downlink packets meant for the user equipment (UE) that is in idle mode.</p> <p>Idle mode buffering uses 1 GB of memory when it is enabled. When it is disabled, this memory is used by the daemon handling subscriber management.</p> <div><p>NOTE: Idle mode buffering can be disabled only when the S-GW is in maintenance mode. When idle mode buffering is changed from enabled to disabled or vice versa, all services PICs of the corresponding S-GW are rebooted.</p></div>
Default	If you do not configure this statement, then idle mode buffering is enabled.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring an S-GW on a Broadband Gateway on page 30• idle-mode-buffering on page 988

expire-timer (Idle Mode Buffering)

Syntax	expire-timer <i>time-in-seconds</i> ;
Hierarchy Level	[edit unified-edge gateways sgw <i>gateway-name</i> idle-mode-buffering]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Configure the expire timer for idle mode buffering in the Serving Gateway (S-GW). After the configured time elapses for a bearer, buffered packets are discarded by the S-GW.
Options	<i>time-in-seconds</i> —Expire timer, in seconds. Default: 200 seconds Range: 30 through 300 seconds
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring an S-GW on a Broadband Gateway on page 30• idle-mode-buffering on page 988


family (Mobile Interface)

Syntax	family <i>family-name</i> {...}
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>interface-unit-number</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the protocol family information for the logical interface.
Options	<i>family-name</i> —Protocol family. The following options are supported: <ul style="list-style-type: none">• inet—IP version 4 suite.• inet6—IP version 6 suite.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Mobile Interfaces for APNs on page 120• unit (Mobile Interface) on page 999

filter (Mobile Interface)

Syntax	<pre>filter { input input-filter; output output-filter; }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>interface-unit-number</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the access control list (ACL) filters to apply to uplink and downlink traffic. By default, the mobile interface (mif)—that is, the access point name (APN)—accepts all mobile traffic of the subscribers that are using this APN (mif).</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Mobile Interfaces for APNs on page 120• unit (Mobile Interface) on page 999

forwarding-packages

Syntax	<pre>forwarding-packages { mobility { ggsn-pgw; sgw; } }</pre>
Hierarchy Level	<pre>[edit chassis fpc <i>fpc-slot</i>], [edit chassis fpc <i>fpc-slot</i> pfe <i>pfe-id</i>]</pre>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the Packet Forwarding Engine so that it can be used to anchor mobile sessions. If this configuration is changed, then the FPC reboots.</p> <p>The forwarding-packages statement can be configured at the Packet Forwarding Engine level. Therefore, you can configure a subset of Packet Forwarding Engines in an FPC to be mobile anchors.</p>
	<div>  <p>NOTE: The configuration at the Packet Forwarding Engine level takes precedence over the configuration at the FPC level.</p> </div>
	The remaining statements are explained separately.
Required Privilege Level	<pre>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</pre>
Related Documentation	<ul style="list-style-type: none"> • Configuring Interface DPCs or MPCs for User Mobility Traffic on page 66 • Example: Configuring the MobileNext Broadband Gateway Chassis on page 67

ggsn-pgw

Syntax	<code>ggsn-pgw gateway-name { ... }</code>
Hierarchy Level	[edit unified-edge gateways]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Specify the name to be used for the broadband gateway. The broadband gateway can be configured as a gateway GPRS support node (GGSN), as a Packet Data Network Gateway (P-GW), or as both a GGSN and a P-GW.</p> <p>The remaining statements are explained separately.</p>
Options	<p>gateway-name—Name of the gateway.</p> <p>Range: Up to 63 characters</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• [edit unified-edge gateways ggsn-pgw <gateway-name>] Hierarchy Level on page 564• Configuring Broadband Gateway Home PLMNs and Gateways on page 11

history (Call-Rate Statistics)

Syntax	<code>history history;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw gateway-name call-rate-statistics], [edit unified-edge gateways sgw gateway-name call-rate-statistics]
Release Information	<p>Statement introduced in Junos OS Mobility Release 11.2W.</p> <p>Support at the [edit unified-edge gateways sgw gateway-name call-rate-statistics] hierarchy level introduced in Junos OS Mobility Release 11.4W.</p>
Description	Configure the number of past intervals for which the call-rate statistics are stored by the broadband gateway.
Options	<p>history—Number of past intervals for which the call-rate statistics are stored.</p> <p>Range: 1 through 20</p> <p>Default: 1</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• call-rate-statistics on page 981• show unified-edge ggsn-pgw call-rate statistics on page 1277• show unified-edge sgw call-rate statistics on page 1282

home-plmn

Syntax	<pre>home-plmn { mcc [mcc] { mnc [mnc]; } }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i>], [edit unified-edge gateways sgw <i>gateway-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i>] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Configure the operator's home public land mobile networks (HPLMNs) that the broadband gateway and its access point names (APNs) recognize. The HPLMN consists of the mobile country code (MCC) and its corresponding mobile network codes (MNCs).



NOTE: Configuring the `home-plmn` statement is optional for the Serving Gateway (S-GW). In order to select the charging profile for a subscriber, the S-GW uses the Serving Network PLMN provided as part of the Serving Network Information Element (IE) in the Create Session Request message. If the Serving Network IE is not available, then the S-GW uses the home PLMN configuration for selecting the charging profile.

The remaining statements are explained separately.

Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Broadband Gateway Home PLMNs and Gateways on page 11 • ggsn-pgw on page 986 • Configuring an S-GW on a Broadband Gateway on page 30

idle-mode-buffering

Syntax	<pre>idle-mode-buffering { disable; expire-timer <i>time-in-seconds</i>; }</pre>
Hierarchy Level	[edit unified-edge gateways <i>sgw gateway-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	<p>Configure the idle mode buffering options for the Serving Gateway (S-GW). When a user equipment (UE) is in idle mode, the S-GW buffers the downlink packets meant for that user equipment.</p> <p>The remaining statements are explained separately.</p>
Default	If you do not configure this statement, then idle mode buffering is enabled with an expire-timer of 200 seconds.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring an S-GW on a Broadband Gateway on page 30• sgw on page 998

input (Mobile Interface)

Syntax	<pre>input <i>input-filter</i>;</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>interface-unit-number</i> filter]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Specify the access control list (ACL) filter to apply to uplink traffic. By default, the mobile interface (mif)—that is, the access point name (APN)—accepts all uplink traffic of the subscribers that are using the APN (mif).</p>
Options	<i>input-filter</i> —Name of the ACL filter.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Mobile Interfaces for APNs on page 120• filter (Mobile Interface) on page 984

interface

Syntax	<code>interface <i>interface-name</i>;</code>
Hierarchy Level	[edit routing-instances], [edit logical-systems logical-system-name routing-instances routing-instance-name]
Release Information	Statement introduced before Junos OS Release 7.4. The option to configure mobile interfaces (mif-) introduced in Junos OS Mobility Release 11.2W.
Description	Configure the mobile interface to access point name (APN) mapping in a virtual routing and forwarding table (VRF) by placing both the mobile interface logical interface unit and the physical interface unit (the Gi or SGi interface for the APN), in the same VRF.
Options	<i>interface-name</i> —Name of the mobile interface logical interface unit or the physical interface unit. For example, mif.1 or ge-0/0/0.5 .
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Mobile Interface to APN Associations in VRFs on page 122

interfaces (Mobile Interface)

Syntax interfaces mif {
 description *description*;
 disable;
 mtu *mtu-size*;
 multi-chassis-protection { ... }
 no-traps;
 traceoptions { ... }
 unit *interface-unit-number*{
 clear-dont-fragment-bit;
 description *description*;
 disable;
 family *family-name* {...}
 filter {
 input *input-filter*;
 output *output-filter*;
 }
 (no-traps | traps);
 }
 }
 }

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the mobile interfaces for access point name (APN) mobile traffic. The mobile interfaces are distinct from other types of interfaces and are used to associate an APN with a physical interface in a virtual routing and forwarding (VRF) table. 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.

The remaining statements are explained separately.


Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Documentation • [Configuring Mobile Interfaces for APNs on page 120](#)

interval (Call-Rate Statistics)

Syntax	<code>interval <i>interval</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> call-rate-statistics], [edit unified-edge gateways sgw <i>gateway-name</i> call-rate-statistics]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> call-rate-statistics] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Configure the interval for which the call-rate statistics are calculated by the broadband gateway.
Options	<i>interval</i> —Interval, in minutes, for which the call-rate statistics are calculated. Range: 5 through 120 minutes Default: 60 minutes
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• call-rate-statistics on page 981• show unified-edge ggsn-pgw call-rate statistics on page 1277• show unified-edge sgw call-rate statistics on page 1282

local-policy-profile (Broadband Gateway)

Syntax	<code>local-policy-profile <i>local-policy-profile</i>;</code>
Hierarchy Level	[edit unified-edge gateways <i>ggsn-pgw gateway-name</i>], [edit unified-edge gateways <i>sgw gateway-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways <i>sgw name</i>] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>Specify a local policy profile for the broadband gateway.</p> <ul style="list-style-type: none">• For the broadband gateway configured as a gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW), the local policy profile is a combination of the quality-of-service (QoS) policy (cos-policy-profile), the classifier policy (classifier-profile), and the resource threshold policy (resource-threshold-policy).• For the broadband gateway configured as a Serving Gateway (S-GW), the local policy profile is a combination of the classifier policy (classifier-profile) and the resource threshold policy (resource-threshold-policy).
	<div><p>NOTE: The local policy profile must already be configured at the [edit unified-edge] hierarchy level.</p></div>
Options	<i>local-policy-profile</i> —Name of the local policy profile.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• local-policy-profile (APN) on page 720 (P-GW only)

maximum-bearers (Broadband Gateway)

Syntax	<code>maximum-bearers <i>maximum-bearers</i>;</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i>], [edit unified-edge gateways sgw <i>gateway-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways <i>sgw name</i>] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	<p>For the broadband gateway configured as a gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW), configure the maximum number of Evolved Packet System (EPS) bearers or packet data protocol (PDP) contexts allowed.</p> <p>For the broadband gateway configured as a Serving Gateway (S-GW), configure the maximum number of EPS bearers allowed.</p>
Options	<p><i>maximum-bearers</i>—Maximum number of bearers for the broadband gateway.</p> <p>Range: 100,000 through 12,000,000 bearers</p> <p>Default: 12,000,000 bearers</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Maximum Number of Bearers on page 324• maximum-bearers (APN) on page 722 (P-GW only)

mcc

Syntax `mcc [mcc] {
 mnc [mnc];
 }`

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name* home-plmn],
 [edit unified-edge gateways sgw *gateway-name* home-plmn]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.
 Support at the [edit unified-edge gateways sgw *gateway-name* home-plmn] hierarchy
 level introduced in Junos OS Mobility Release 11.4W.

Description Configure the mobile country codes (MCCs) for the operator's home public land mobile
 networks (HPLMNs) that the broadband gateway and its access point names (APNs)
 recognize. For each MCC, you can configure a list of mobile network codes (MNCs).



NOTE: This is a mandatory configuration for the gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW).

The remaining statement is explained separately.

Options *mcc*—Mobile country code.

Syntax: The MCC must be three digits long and can contain numbers from 0 through 9.



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

To configure multiple MCCs, include the **mcc** statement multiple times.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring Broadband Gateway Home PLMNs and Gateways on page 11](#)
- [home-plmn on page 987](#)
- [Configuring an S-GW on a Broadband Gateway on page 30](#)

mnc

Syntax	<code>mnc [mnc];</code>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> home-plmn mcc], [edit unified-edge gateways sgw <i>gateway-name</i> home-plmn mcc]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i> home-plmn mcc] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Configure the mobile network codes (MNCs) belonging to the mobile country codes (MCCs) for the operator's home public land mobile networks (HPLMNs) that the broadband gateway and its access point names (APNs) recognize.



NOTE: This is a mandatory configuration for the gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW).

Options `mnc`—Mobile network code.

Syntax: The MNC must be at least two digits long and a maximum of three digits long. It can contain numbers from 0 through 9.



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


To configure multiple MNCs, include the `mnc` statement multiple times.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring Broadband Gateway Home PLMNs and Gateways on page 11](#)
- [mcc on page 994](#)
- [Configuring an S-GW on a Broadband Gateway on page 30](#)

mobility

Syntax	<pre>mobility { ggsn-pgw; sgw; }</pre>
Hierarchy Level	[edit chassis fpc <i>fpc-slot</i> forwarding-packages], [edit chassis fpc <i>fpc-slot</i> pfe <i>pfe-id</i> forwarding-packages]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. sgw statement introduced in Junos OS Mobility Release 11.4W.
Description	<p>Specify the forwarding package that the Packet Forwarding Engines associated with mobility must use. You can configure the forwarding package in the following ways:</p> <ul style="list-style-type: none"> For an FPC, so that all the Packet Forwarding Engines on the FPC are configured with the same forwarding package. For an individual Packet Forwarding Engine.
	<div>  <p>NOTE:</p> <ul style="list-style-type: none"> 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. 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. </div>
Options	<p>ggsn-pgw—Configure the router as a gateway GPRS support node (GGSN) or as a Packet Data Network Gateway (P-GW).</p> <p>sgw—Configure the router as a Serving Gateway (S-GW).</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring Interface DPCs or MPCs for User Mobility Traffic on page 66 Example: Configuring the MobileNext Broadband Gateway Chassis on page 67 forwarding-packages on page 985

mtu (Mobile Interface)

Syntax	<code>mtu <i>mtu-size</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Configure the maximum transmission unit (MTU) size for the mobile interface. MTU sizes can be important because the GPRS tunneling protocol (GTP) tunneling can cause a data unit to exceed the maximum frame size when the tunnel headers are added, which causes an error. However, larger MTU sizes increase throughput.
Options	<i>mtu-size</i> —MTU size. Range: 256 through 9192 bytes Default: 500 bytes (INET, INET6, and ISO families), 1448 bytes (MPLS)
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Mobile Interfaces for APNs on page 120• interfaces (Mobile Interface) on page 990

output (Mobile Interface)

Syntax	<code>output <i>output-filter</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>interface-unit-number</i> filter]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Specify the access control list (ACL) filter to apply to downlink traffic. By default, the mobile interface (mif)—that is, the access point name (APN)—accepts all downlink traffic of the subscribers that are using the APN (mif).
Options	<i>output-filter</i> —Name of the ACL filter.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Mobile Interfaces for APNs on page 120• filter (Mobile Interface) on page 984

remote-delete-on-peer-fail

Syntax	remote-delete-on-peer-fail;
Hierarchy Level	[edit unified-edge gateways <i>sgw gateway-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Specify that the Serving Gateway (S-GW) sends a delete message to the Packet Data Network Gateway (P-GW) when the S-GW detects that a peer has failed.
Default	If you do not include the remote-delete-on-peer-fail statement, then the S-GW only deletes the packet data protocol (PDP) contexts or bearers locally on the S-GW.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring an S-GW on a Broadband Gateway on page 30• sgw on page 998

sgw

Syntax	<i>sgw gateway-name</i> { ... }
Hierarchy Level	[edit unified-edge gateways]
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Specify the name to be used for the Serving Gateway (S-GW). The remaining statements are explained separately.
Options	<i>gateway-name</i> —Name of the gateway. Range: Up to 63 characters in length.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• [edit unified-edge gateways <i>sgw <gateway-name></i>] Hierarchy Level on page 574• Configuring an S-GW on a Broadband Gateway on page 30

unit (Mobile Interface)

Syntax	<pre> unit <i>interface-unit-number</i>{ clear-dont-fragment-bit; description <i>description</i>; disable; family <i>family-name</i> {...} filter { input <i>input-filter</i>; output <i>output-filter</i>; } (no-traps traps); } </pre>
Hierarchy Level	[edit interfaces <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Configure the logical interface on the physical device. You must configure a logical interface to be able to use the physical device.</p> <p>The remaining statements are explained separately.</p>
Options	<p><i>interface-unit-number</i>—Number of the logical unit.</p> <p>Range: 0 through 16,384</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Mobile Interfaces for APNs on page 120 • interfaces (Mobile Interface) on page 990

Gateway Traceoptions Configuration Statements

client (Resource Management)

Syntax

```
client {  
  traceoptions {  
    file filename {  
      files files;  
      match match;  
      (no-world-readable | world-readable);  
      size size;  
    }  
    flag {  
      flag;  
    }  
    level level;  
    no-remote-trace;  
  }  
}
```

Hierarchy Level [edit unified-edge resource-management]

Description Define the tracing options for the resource management client (the session Dense Port Concentrators [DPCs] and interface DPCs and Modular Port Concentrators [MPCs]). Resource management tracing operations record detailed messages about the operation of resource management clients on the broadband gateway.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring Resource Manager Trace Options on page 19](#)
- [resource-management \(MobileNext Broadband Gateway\) on page 1002](#)

mobile-options

Syntax	<pre>mobile-options { traceoptions { file <i>filename</i> { files <i>files</i>; match <i>match</i>; (no-world-readable world-readable); size <i>size</i>; } flag { <i>flag</i>; } no-remote-trace; } }</pre>
Hierarchy Level	[edit unified-edge]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Specify the tracing options for the mobility daemon.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • [edit unified-edge] Hierarchy Level on page 559 • Configuring Mobile Options Trace Options on page 17

resource-management (MobileNext Broadband Gateway)

```
Syntax  resource-management {  
        client {  
            traceoptions {  
                file filename {  
                    files files;  
                    match match;  
                    (no-world-readable | world-readable);  
                    size size;  
                }  
            }  
            flag {  
                flag;  
            }  
            level level;  
            no-remote-trace;  
        }  
    }  
    server {  
        traceoptions {  
            file filename {  
                files files;  
                match match;  
                (no-world-readable | world-readable);  
                size size;  
            }  
        }  
        flag {  
            flag;  
        }  
        level level;  
        no-remote-trace;  
    }  
}
```

Hierarchy Level [edit unified-edge]

Description Define the resource management tracing options. Resource management tracing operations record detailed messages about the operation of resource management clients and server on the broadband gateway.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [\[edit unified-edge\] Hierarchy Level on page 559](#)
- [Configuring Resource Manager Trace Options on page 19](#)

server (Resource Management)

```
Syntax  server {
        traceoptions {
            file filename {
                files files;
                match match;
                (no-world-readable | world-readable);
                size size;
            }
            flag {
                flag;
            }
            level level;
            no-remote-trace;
        }
    }
```

Hierarchy Level [edit unified-edge resource-management]

Description Define the tracing options for the resource management server (the active Routing Engine). Resource management tracing operations record detailed messages about the operation of the resource management server on the broadband gateway.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring Resource Manager Trace Options on page 19](#)
- [resource-management \(MobileNext Broadband Gateway\) on page 1002](#)

traceoptions (Broadband Gateway)

Syntax	<pre>traceoptions { file <i>filename</i> { files <i>files</i>; match <i>match</i>; (no-world-readable world-readable); size <i>size</i>; } flag { <i>flag</i>; } level <i>level</i>; no-remote-trace; }</pre>
Hierarchy Level	[edit unified-edge gateways ggsn-pgw <i>gateway-name</i>], [edit unified-edge gateways sgw <i>gateway-name</i>]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W. Support at the [edit unified-edge gateways sgw <i>gateway-name</i>] hierarchy level introduced in Junos OS Mobility Release 11.4W.
Description	Define the tracing operations for the broadband gateway. You can specify which trace operations are logged by including specific tracing flags and levels.
Options	<p>file <i>filename</i>—Name of the file that receives the output of the tracing operation. All files are placed in the <code>/var/log</code> directory.</p> <p>files <i>files</i>— (Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you must also specify a maximum file size with the size option and a filename.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag</p> <ul style="list-style-type: none">• <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can use one of the following flags:<ul style="list-style-type: none">• all—Trace everything.• bulkjob—Trace events that are handled by bulk jobs in order to prevent system overload.• config—Trace configuration events.• cos-cac—Trace class of service (CoS) and call admission control (CAC) events.

- **ctxt**—Trace user equipment, Packet Data Network (PDN), or bearer context events.
- **fsm**—Trace mobile subscriber finite state machine (FSM) events.
- **gtpu**—Trace GPRS tunneling protocol, user plane (GTP-U) events.
- **ha**—Trace high availability events.
- **init**—Trace initialization events.
- **pfem**—Trace Packet Forwarding Engine Manager events.
- **stats**—Trace **stats** events. This flag is used internally by Juniper's engineers.
- **waitq**—Trace **waitq** events. This flag is used internally by Juniper's engineers.

level *level*—(Optional) Level of tracing to perform. You can specify any of the following levels:

- **all**—Match all levels.
- **critical**—Match critical conditions.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match conditions that should be handled specially
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

match *match*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—(Optional) Disable remote tracing.

no-world-readable—(Optional) Restrict access to the originator of the trace operation only.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you must also specify a maximum number of trace files with the **files** option and filename.

Syntax: **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.

- Related Documentation**
- [\[edit unified-edge gateways\] Hierarchy Level on page 563](#)
 - [Configuring General Gateway Trace Options on page 15](#)
 - [Configuring S-GW Traceoptions on page 33](#)

traceoptions (Mobile Options)

Syntax	<pre> traceoptions { file <i>filename</i> { files <i>files</i>; match <i>match</i>; (no-world-readable world-readable); size <i>size</i>; } flag { <i>flag</i>; } no-remote-trace; } </pre>
Hierarchy Level	[edit unified-edge mobile-options]
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	<p>Define the tracing options for the mobility daemon.</p> <p>Tracing options record detailed messages about the operation of the mobility daemon. You can specify which trace operations are logged by including specific tracing flags and levels.</p>
Options	<p>file <i>filename</i>—Name of the file that receives the output of the tracing operation. All files are placed in the <code>/var/log</code> directory.</p> <p>files <i>files</i>— (Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you must also specify a maximum file size with the size option and a filename.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag</p> <ul style="list-style-type: none"> • <i>flag</i>—You can use one of the following flags: <ul style="list-style-type: none"> • all—Trace everything for the mobility daemon. • configuration—Trace configuration commands. • error—Trace events related to errors in the daemon. • init—Trace events related to the protocol initialization daemon. • protocol—Trace protocol processing events.

match *match*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—(Optional) Disable remote tracing.

no-world-readable—(Optional) Restrict access to the originator of the trace operation only.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you must also specify a maximum number of trace files with the **files** option and filename.

Syntax: **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level	interface—To view this statement in the configuration.
	interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Mobile Options Trace Options on page 17• mobile-options on page 1001

traceoptions (Resource Management Client)

Syntax

```

traceoptions {
    file filename {
        files files;
        match match;
        (no-world-readable | world-readable);
        size size;
    }
    flag {
        flag;
    }
    level level;
    no-remote-trace;
}

```

Hierarchy Level [edit unified-edge resource-management client]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Define the tracing options for the resource management client (the session Dense Port Concentrators [DPCs] and interface DPCs and Modular Port Concentrators [MPCs]). Resource management tracing operations record detailed messages about the operation of resource management clients on the broadband gateway. You can specify which trace operations are logged by including specific tracing flags and levels.

Options **file *filename***—Name of the file that receives the output of the tracing operation. All files are placed in the `/var/log` directory.



NOTE: The FPC and PIC slot numbers are appended to the specified filename to obtain a unique filename for each DPC.

files *files*— (Optional) Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.

If you specify a maximum number of files, you must also specify a maximum file size with the **size** option and a filename.

Range: 2 through 1000

Default: 3 files

flag

- ***flag***—You can use one of the following flags:



NOTE: Currently, only the **all** flag is supported. The other flags are not fully supported.

- **all**—Trace everything.
- **communication**—Trace Inter-Process Communication (IPC) code.
- **info-tables**—Trace information table code.
- **infra**—Trace finite state machine (FSM) and infra code.
- **memory**—Trace memory management code.
- **redundancy**—Trace graceful Routing Engine switchover (GRES) code.
- **resource-tables**—Trace resource table code.

level *level*—(Optional) Level of tracing to perform. You can specify any of the following levels:

- **all**—Match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match conditions that should be handled specially
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

match *match*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—(Optional) Disable remote tracing.

no-world-readable—(Optional) Restrict access to the originator of the trace operation only.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you must also specify a maximum number of trace files with the **files** option and filename.

Syntax: **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.

- Related Documentation**
- [client \(Resource Management\) on page 1000](#)
 - [Configuring Resource Manager Trace Options on page 19](#)

traceoptions (Resource Management Server)

Syntax `traceoptions {
 file filename {
 files files;
 match match;
 (no-world-readable | world-readable);
 size size;
 }
 flag {
 flag;
 }
 level level;
 no-remote-trace;
 }`

Hierarchy Level [edit unified-edge resource-management server]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Define the tracing options for the resource management server (the active Routing Engine). Resource management tracing operations record detailed messages about the operation of the resource management server on the broadband gateway. You can specify which trace operations are logged by including specific tracing flags and levels.

Options **file *filename***—Name of the file that receives the output of the tracing operation. All files are placed in the `/var/log` directory.



.....
NOTE: The FPC and PIC slot numbers are appended to the specified filename to obtain a unique filename for each DPC.
.....

files *files*— (Optional) Maximum number of trace files. When a trace file named **trace-file** reaches its maximum size, it is renamed **trace-file.0**, then **trace-file.1**, and so on, until the maximum number of trace files is reached. Then, the oldest trace file is overwritten.

If you specify a maximum number of files, you must also specify a maximum file size with the **size** option and a filename.

Range: 2 through 1000

Default: 3 files

flag

- **flag**—You can use one of the following flags:



.....
NOTE: Currently, only the all flag is supported. The other flags are not fully supported.
.....

- **all**—Trace everything.
- **communication**—Trace infra code.
- **configuration**—Trace configuration code.
- **gres**—Trace graceful Routing Engine switchover (GRES) code.
- **info-manager**—Trace information management code.
- **init**—Trace events related to the Resource Management and Packet Steering Daemon(RMPSD) initialization sequence of messages.
- **memory**—Trace memory management code.
- **packet-steering**—Trace packet-steering code.
- **resource-manager**—Trace resource management code.
- **signal**—Trace signal-handling code.
- **state**—Trace state-handling code.
- **timer**—Trace timer code.
- **ui**—Trace user interface code.

level *level*—(Optional) Level of tracing to perform. You can specify any of the following levels:

- **all**—Match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match conditions that should be handled specially
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

match *match*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—(Optional) Disable remote tracing.

no-world-readable—(Optional) Restrict access to the originator of the trace operation only.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you must also specify a maximum number of trace files with the **files** option and filename.

Syntax: **xk** to specify KB, **xm** to specify MB, or **xg** to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.

Related Documentation	<ul style="list-style-type: none">• Configuring Resource Manager Trace Options on page 19• server (Resource Management) on page 1003
------------------------------	---

PART 12

Command Reference

- [AAA Operational Commands on page 1017](#)
- [Anchor Packet Forwarding Engine Redundancy and Aggregated Multiservices High Availability Operational Commands on page 1053](#)
- [APN and Related Operational Commands on page 1071](#)
- [Charging Operational Commands on page 1109](#)
- [Class of Service \(CoS\) Operational Commands on page 1173](#)
- [Exception Handling Operational Commands on page 1183](#)
- [GPRS Tunneling Protocol \(GTP\) Operational Commands on page 1193](#)
- [Service Applications Operational Commands on page 1237](#)
- [System Architecture Operational Commands on page 1269](#)

CHAPTER 29

AAA Operational Commands

clear unified-edge ggsn-pgw aaa radius statistics

Syntax	<code>clear unified-edge ggsn-pgw aaa radius statistics (accounting all authentication dynamic-requests)</code> <code><fpc-slot fpc-slot></code> <code><gateway-name gateway-name></code> <code><name name></code> <code><pic-slot pic-slot></code>
Release Information	Command introduced in Junos OS Mobility Release 11.2W. gateway-name option introduced in Junos OS Mobility Release 11.4W.
Description	Clear statistics for the authentication, authorization, and accounting (AAA) RADIUS server for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then statistics for all GGSNs and P-GWs are cleared.
Options	accounting all authentication dynamic-requests —Clear statistics for the specified parameter. fpc-slot fpc-slot —(Optional) Clear the statistics for the specified Flexible PIC Concentrator (FPC). gateway-name gateway-name —(Optional) Clear the statistics for the specified GGSN or P-GW. name name —(Optional) Clear the statistics for the specified server. pic-slot pic-slot —(Optional) Clear the statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show unified-edge ggsn-pgw aaa radius statistics on page 1026
List of Sample Output	clear unified-edge ggsn-pgw aaa radius statistics all on page 1018
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

<code>clear unified-edge ggsn-pgw aaa radius statistics all</code>	<code>user@host> clear unified-edge ggsn-pgw aaa radius statistics all</code>
	Cleared all RADIUS statistics

clear unified-edge ggsn-pgw aaa statistics

Syntax	clear unified-edge ggsn-pgw aaa statistics (accounting all authentication dynamic-requests)) <fpc-slot <i>fpc-slot</i> > <gateway-name <i>gateway-name</i> > <pic-slot <i>pic-slot</i> >
Release Information	Command introduced in Junos OS Mobility Release 11.2W. gateway-name option introduced in Junos OS Mobility Release 11.4W.
Description	Clear the global authentication, authorization, and accounting (AAA) statistics for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then statistics for all GGSNs and P-GWs are cleared.
Options	<p>accounting all authentication dynamic-requests—Clear statistics for the specified parameter.</p> <p>fpc-slot <i>fpc-slot</i>—(Optional) Clear the statistics for the specified Flexible PIC Concentrator (FPC).</p> <p>gateway-name <i>gateway-name</i>—(Optional) Clear the statistics for the specified GGSN or P-GW.</p> <p>pic-slot <i>pic-slot</i>—(Optional) Clear the statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show unified-edge ggsn-pgw aaa radius statistics on page 1026
List of Sample Output	clear unified-edge ggsn-pgw aaa statistics all on page 1019
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
clear unified-edge ggsn-pgw aaa statistics all
user@host> clear unified-edge ggsn-pgw aaa statistics all
Cleared all AAA statistics
```

clear unified-edge ggsn-pgw address-assignment pool

Syntax	<code>clear unified-edge ggsn-pgw address-assignment pool name <i>pool-name</i></code> <code><gateway <i>gateway</i>></code> <code><routing-instance <i>routing-instance</i>></code>
Release Information	Command introduced in Junos OS Mobility Release 11.2W. <code>gateway</code> option introduced in Junos OS Mobility Release 11.4W.
Description	Clear the sessions that have been assigned addresses from the specified mobile pool for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then the sessions for all GGSNs and P-GWs are cleared.
Options	<code>name <i>pool-name</i></code> —Clear the sessions for the specified mobile pool. <code>gateway <i>gateway</i></code> —(Optional) Clear the sessions on the specified GGSN or P-GW. <code>routing-instance <i>routing-instance</i></code> —(Optional) Clear the sessions on the specified routing instance.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show unified-edge ggsn-pgw address-assignment pool on page 1044
List of Sample Output	clear unified-edge ggsn-pgw address-assignment pool name pool-1 on page 1020
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

<code>clear unified-edge ggsn-pgw address-assignment pool name pool-1</code>	<pre>user@host> clear unified-edge ggsn-pgw address-assignment pool name pool-1 Initiated clearing of sessions in the pool</pre>
--	---

clear unified-edge ggsn-pgw address-assignment statistics

Syntax	<code>clear unified-edge ggsn-pgw address-assignment statistics</code> <code><fpc-slot <i>fpc-slot</i>></code> <code><gateway <i>gateway</i>></code> <code><pic-slot <i>pic-slot</i>></code>
Release Information	Command introduced in Junos OS Mobility Release 11.2W. gateway option introduced in Junos OS Mobility Release 11.4W.
Description	Clear the global address assignment statistics for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then the statistics for all GGSNs and P-GWs are cleared.
Options	fpc-slot <i>fpc-slot</i> pic-slot <i>pic-slot</i> —(Optional) Clear the statistics for the services PIC in the specified FPC and PIC slots. gateway <i>gateway</i> —(Optional) Clear the statistics for the specified GGSN or P-GW.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show unified-edge ggsn-pgw address-assignment statistics on page 1050
List of Sample Output	clear unified-edge ggsn-pgw address-assignment statistics on page 1021
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

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

show unified-edge ggsn-pgw aaa network-element status

Syntax	<pre>show unified-edge ggsn-pgw aaa network-element status <fpc-slot fpc-slot> <gateway-name gateway-name> <name name> <pic-slot pic-slot></pre>
Release Information	<p>Command introduced in Junos OS Mobility Release 11.2W.</p> <p>gateway-name option introduced in Junos OS Mobility Release 11.4W.</p>
Description	<p>Display the authentication, authorization, and accounting (AAA) network element status for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then the status for all GGSNs and P-GWs is displayed.</p>
Options	<p>none—Display the network element group status for all the GGSNs or P-GWs.</p> <p>fpc-slot fpc-slot—(Optional) Display the status for the specified Flexible PIC Concentrator (FPC).</p> <p>gateway-name gateway-name—(Optional) Display the status for the specified GGSN or P-GW.</p> <p>name name—(Optional) Display the status for the specified network element.</p> <p>pic-slot pic-slot—(Optional) Display the status for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show unified-edge ggsn-pgw aaa network-element-group status on page 1024
List of Sample Output	show unified-edge ggsn-pgw aaa network-element status on page 1023
Output Fields	<p>Table 57 on page 1022 lists the output fields for the show unified-edge ggsn-pgw aaa network-element status command. Output fields are listed in the approximate order in which they appear.</p>

Table 57: show unified-edge ggsn-pgw aaa network-element status Output Fields

Field Name	Field Description
Server	Name of the RADIUS server that is part of the network element.
FPC/PIC	FPC and PIC slot numbers through which the network element was reached.
Priority	Priority of the RADIUS server in the network element. Within a network element, a RADIUS server can be assigned a priority of 1 or 2.

Table 57: show unified-edge ggsn-pgw aaa network-element status Output Fields (*continued*)

Field Name	Field Description
State	State of the RADIUS server: dead or active.

Sample Output

```
show unified-edge ggsn-pgw aaa network-element status
user@host> show unified-edge ggsn-pgw aaa network-element status
Network-element: rad (FPC/PIC: 4/0)
  Server: rad, Priority: 1, State: Active
Network-element: rad1 (FPC/PIC: 4/0)
  Server: rad1, Priority: 1, State: Active
```

show unified-edge ggsn-pgw aaa network-element-group status

Syntax	<pre>show unified-edge ggsn-pgw aaa network-element-group status <brief detail> <fpc-slot fpc-slot> <gateway-name name> <name name> <pic-slot pic-slot></pre>
Release Information	<p>Command introduced in Junos OS Mobility Release 11.2W.</p> <p>gateway-name option introduced in Junos OS Mobility Release 11.4W.</p>
Description	Display the authentication, authorization, and accounting (AAA) network element group status for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then the status for all GGSNs and P-GWs is displayed.
Options	<p>none—(Same as brief) Display the network element group status in brief.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>fpc-slot fpc-slot—(Optional) Display the status for the specified Flexible PIC Concentrator (FPC).</p> <p>gateway-name name—(Optional) Display the status for the specified GGSN or P-GW.</p> <p>name name—(Optional) Display the status for the specified network element group.</p> <p>pic-slot pic-slot—(Optional) Display the status for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show unified-edge ggsn-pgw aaa network-element status on page 1022
List of Sample Output	<p>show unified-edge ggsn-pgw aaa network-element-group status brief on page 1025</p> <p>show unified-edge ggsn-pgw aaa network-element-group status detail on page 1025</p>
Output Fields	Table 58 on page 1024 lists the output fields for the show unified-edge ggsn-pgw aaa network-element-group status command. Output fields are listed in the approximate order in which they appear.

Table 58: show unified-edge ggsn-pgw aaa network-element-group status Output Fields

Field Name	Field Description
network element-group	Name of the network element group.
Broadcast	Indicates whether the broadcast knob has been enabled for this network element group. If the broadcast knob is enabled, the broadband gateway can broadcast accounting messages to all of the network elements in the group.

Table 58: show unified-edge ggsn-pgw aaa network-element-group status Output Fields (*continued*)

Field Name	Field Description
Members	Members of the network element group and their mandatory status in the group.

Sample Output

```

show unified-edge user@host> show unified-edge ggsn-pgw aaa network-element-group status brief
ggsn-pgw aaa
network-element-group network element-group: NEG_1
status brief          Broadcast: Disabled
                      Members:
                        ne1, Mandatory: No
                        ne2, Mandatory: No

                      network element-group: NEG_2
                      Broadcast: Enabled
                      Members:
                        ne1, Mandatory: Yes
                        ne2, Mandatory: No

                      network element-group: ne_group1
                      Broadcast: Enabled
                      Members:
                        ne1, Mandatory: No
                        ne2, Mandatory: Yes

show unified-edge user@host> show unified-edge ggsn-pgw aaa network-element-group status detail
ggsn-pgw aaa
network-element-group network element-group: NEG_1
status detail          Broadcast: Disabled
                      Members:
                        ne1, Mandatory: No
                        ne2, Mandatory: No

```

[show unified-edge ggsn-pgw aaa radius statistics](#)

Syntax	<code>show unified-edge ggsn-pgw aaa radius statistics (authentication accounting dynamic-requests) <brief detail summary> <fpc-slot <i>fpc-slot</i>> <gateway-name <i>gateway-name</i>> <name <i>name</i>> <pic-slot <i>pic-slot</i>></code>
Release Information	Command introduced in Junos OS Mobility Release 11.2W. gateway-name option introduced in Junos OS Mobility Release 11.4W.
Description	Display the statistics for the authentication, authorization, and accounting (AAA) RADIUS server for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then statistics for all GGSNs and P-GWs is displayed.
Options	authentication accounting dynamic-requests —Display the statistics for the specified parameter. brief detail summary —(Optional) Display the specified level of output. fpc-slot <i>fpc-slot</i> —(Optional) Display the statistics for the specified Flexible PIC Concentrator (FPC). gateway-name <i>gateway-name</i> —(Optional) Display the statistics for the specified GGSN or P-GW. name <i>name</i> —(Optional) Display the statistics for the specified RADIUS server. pic-slot <i>pic-slot</i> —(Optional) Display the statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• clear unified-edge ggsn-pgw aaa radius statistics on page 1018• show unified-edge ggsn-pgw aaa statistics on page 1035
List of Sample Output	show unified-edge ggsn-pgw aaa radius statistics accounting brief on page 1030 show unified-edge ggsn-pgw aaa radius statistics accounting detail on page 1030 show unified-edge ggsn-pgw aaa radius statistics accounting summary on page 1031 show unified-edge ggsn-pgw aaa radius statistics authentication brief on page 1031 show unified-edge ggsn-pgw aaa radius statistics authentication detail on page 1031 show unified-edge ggsn-pgw aaa radius statistics authentication summary on page 1032 show unified-edge ggsn-pgw aaa radius statistics dynamic-requests brief on page 1032 show unified-edge ggsn-pgw aaa radius statistics dynamic-requests detail on page 1032 show unified-edge ggsn-pgw aaa radius statistics dynamic-requests summary on page 1033

Output Fields Table 59 on page 1027 lists the output fields for the **show unified-edge ggsn-pgw aaa radius statistics** command. Output fields are listed in the approximate order in which they appear.

Table 59: show unified-edge ggsn-pgw aaa radius statistics Output Fields

Field Name	Field Description	Level of Output
------------	-------------------	-----------------

The following statistics are displayed only when this command is executed with either the **accounting** or **authentication** options.

RADIUS server	Name of the RADIUS server.	All levels
Address	IP address of the RADIUS server.	All levels
Port	Port number of the RADIUS server.	All levels
FPC/PIC	FPC and PIC slot numbers for which the statistics are displayed.	All levels
Routing-instance	Routing instance under which the RADIUS server is configured.	detail
State	State of the RADIUS server, that is, whether the server is active or inactive (dead).	All levels
Duration	Duration, in HH:MM:SS format, for which the RADIUS server has been in the current state.	All levels
Previous duration or Prev duration	Duration, in HH:MM:SS format, for which the RADIUS server was in the previous state.	All levels
Flaps	Number of times that the RADIUS server transitioned from the active to inactive state.	All levels

The following statistics are displayed only when this command is executed with the **accounting** option.

Requests	Number of accounting requests sent to the RADIUS server from the FPC slot and PIC slot.	brief summary
Accounting Requests	Number of accounting requests sent to the RADIUS server from the FPC slot and PIC slot. The following information is displayed about each request type: <ul style="list-style-type: none"> • Start—Number of Accounting Start requests sent. • Stop—Number of Accounting Stop requests sent. • Interim—Number of Accounting Interim-Update requests sent. • On—Number of Accounting On requests sent. • Off—Number of Accounting Off requests sent. 	detail
Accounting req retransmissions	Number of accounting requests retransmitted to the RADIUS server.	detail
Responses or Accounting Responses	Number of accounting responses received from the RADIUS server.	All levels

Table 59: show unified-edge ggsn-pgw aaa radius statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
Malformed responses	Number of malformed accounting responses received from the RADIUS server.	detail
Bad authenticators	Number of responses received from the RADIUS server with bad authenticators.	detail
Pending requests	Number of accounting requests waiting for responses from the RADIUS server.	detail
Timeouts	Number of accounting requests to the RADIUS server that timed out.	detail
Unknown types	Number of unknown type responses (that the gateway does not recognize) received from the RADIUS server.	detail
Packets dropped	Number of packets dropped.	detail
Round trip time (ms)	Time taken to receive the response from the RADIUS server. The minimum, average, and maximum round-trip times are also displayed.	detail
Time since counters were last cleared	Time, in hours, minutes, and seconds, since the accounting counters were last cleared.	detail
The following statistics are displayed only when this command is executed with the authentication option.		
Requests	Number of access requests sent to the RADIUS server from the FPC slot and PIC slot.	brief summary
Access req retransmissions	Number of access requests retransmitted to the RADIUS server.	detail
Access rejects	Number of access requests rejected by the RADIUS server.	All levels
Access challenges	Number of Access Challenge responses received from the RADIUS server.	detail
Malformed responses	Number of malformed access responses received from the RADIUS server.	detail
Bad authenticators	Number of bad authentication responses received.	detail
Pending requests	Number of access requests waiting for responses from the RADIUS server.	detail
Timeouts	Number of access requests to the RADIUS server that timed out.	detail
Unknown types	Number of unknown type responses (that the gateway does not recognize) received from the RADIUS server.	detail
Packets dropped	Number of packets dropped.	detail

Table 59: show unified-edge ggsn-pgw aaa radius statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
Round trip time (ms)	Time taken to receive the response from the RADIUS server. The minimum, average, and maximum round-trip times are also displayed.	detail
Time since counters were last cleared	Time, in hours, minutes, and seconds, since the authentication counters were last cleared.	detail
The following statistics are displayed only when this command is executed with the dynamic-requests option.		
RADIUS client	Name of the RADIUS client.	All levels
Address	IP address of the RADIUS client.	All levels
CoA requests received	Number of Change of Authorization (COA) requests received from the RADIUS client.	All levels
DM requests received	Number of Disconnect Message (DM) requests received from the RADIUS client.	All levels
CoA Acks sent	Number of COA acknowledgements sent to the RADIUS client.	All levels
CoA Nacks sent	Number of COA negative acknowledgements sent to the RADIUS client.	All levels
DM Acks sent	Number of Disconnect Message acknowledgements sent to the RADIUS client.	All levels
DM Nacks sent	Number of Disconnect Message negative acknowledgements sent to the RADIUS client.	All levels
Dropped	Number of dynamic authorization requests dropped.	All levels
Duplicates	Number of duplicate dynamic authorization requests.	detail
Forwarded	Number of dynamic authorization requests that were forwarded.	detail
Timeouts	Number of dynamic authorization requests that timed out.	detail
Delivered	Number of dynamic authorization requests that were delivered.	detail
Invalid RADIUS codes	Number of dynamic authorization requests with invalid RADIUS codes.	detail
Errors during processing	Number of dynamic authorization requests that could not be processed due to errors.	detail
Invalid RADIUS authenticators	Number of dynamic authorization requests with invalid RADIUS authenticators.	detail

Table 59: show unified-edge ggsn-pgw aaa radius statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
Invalid or missing Charging Ids	Number of dynamic authorization requests with invalid charging IDs or that did not contain charging IDs.	detail
Session mapping errors	Number of dynamic authorization requests that caused session mapping errors during processing.	detail
Time since counters were last cleared	Time, in hours, minutes, and seconds, since the dynamic requests counters were last cleared.	detail

Sample Output

```

show unified-edge ggsn-pgw aaa radius statistics accounting brief
user@host> show unified-edge ggsn-pgw aaa radius statistics accounting brief

RADIUS server: rad1
Address: 7.1.1.2 Port: 1813
FPC/

```

PIC	State	Duration	Previous Duration	Flaps	Requests	Responses
2/1	Active	00:52:03	00:00:00	0	0	0

```

RADIUS server: radius_server
Address: 4.1.1.2 Port: 1813
FPC/

```

PIC	State	Duration	Previous Duration	Flaps	Requests	Responses
2/1	Active	00:52:03	00:00:00	0	10001	10001

```

show unified-edge ggsn-pgw aaa radius statistics accounting detail
user@host> show unified-edge ggsn-pgw aaa radius statistics accounting detail

RADIUS server: rad1 (FPC/PIC: 2/1)
Address: 7.1.1.2 Port: 1813
Routing-instance: default
State: Active Duration: 00:53:47
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

```

```

RADIUS server: radius_server (FPC/PIC: 2/1)
Address: 4.1.1.2 Port: 1813
Routing-instance: default
State: Active Duration: 00:53:47
Prev duration: 00:00:00 Flaps: 0
Accounting requests: 10001
Start: 10001 Stop: 0 Interim: 0 On: 0 Off: 0
Accounting req retransmissions: 0
Accounting responses: 10001

```

```

Malformed responses: 0
Bad authenticators: 0
Pending requests: 0
Timeouts: 0
Unknown types: 0
Packets dropped: 0
Round trip time (ms): 1 (Min: 0 Max: 14 Avg: 1)
Time since counters were last cleared: 00:00:00

```

**show unified-edge
ggsn-pgw aaa radius
statistics accounting
summary**

```
user@host> show unified-edge ggsn-pgw aaa radius statistics accounting summary
```

```

RADIUS server: rad1
Address: 7.1.1.2 Port: 1813
FPC/
PIC State      Duration      Previous
2/1 Active     00:54:14     00:00:00    0    0    0

```

```

RADIUS server: radius_server
Address: 4.1.1.2 Port: 1813
FPC/
PIC State      Duration      Previous
2/1 Active     00:54:14     00:00:00    0   10001 10001

```

**show unified-edge
ggsn-pgw aaa radius
statistics
authentication brief**

```
user@host> show unified-edge ggsn-pgw aaa radius statistics authentication brief
```

```

RADIUS server: rad1
Address: 7.1.1.2 Port: 1812
FPC/
PIC State      Duration      Previous
2/1 Active     00:54:36     00:00:00    0   10003 10003

```

```

RADIUS server: radius_server
Address: 4.1.1.2 Port: 1812
FPC/
PIC State      Duration      Previous
2/1 Active     00:54:36     00:00:00    0   10001 10001

```

**show unified-edge
ggsn-pgw aaa radius
statistics
authentication detail**

```
user@host> show unified-edge ggsn-pgw aaa radius statistics authentication detail
```

```

RADIUS server: rad1 (FPC/PIC: 2/1)
Address: 7.1.1.2 Port: 1812
Routing-instance: default
State: Active Duration: 00:54:40
Prev duration: 00:00:00 Flaps: 0
Access requests: 10003
Access req retransmissions: 1811
Access accepts: 10003
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): 1 (Min: 0 Max: 25 Avg: 2)
Time since counters were last cleared: 00:00:00

```

```

RADIUS server: radius_server (FPC/PIC: 2/1)
Address: 4.1.1.2 Port: 1812
Routing-instance: default
State: Active Duration: 00:54:40
Prev duration: 00:00:00 Flaps: 0
Access requests: 10001
Access req retransmissions: 1
Access accepts: 10001
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): 1 (Min: 0 Max: 34 Avg: 1)
Time since counters were last cleared: 00:00:00

```

**show unified-edge
ggsn-pgw aaa radius
statistics
authentication
summary**

```
user@host> show unified-edge ggsn-pgw aaa radius statistics authentication summary
```

```

RADIUS server: rad1
Address: 7.1.1.2 Port: 1812
FPC/
PIC State      Duration      Previous
2/1 Active     00:54:45     Duration Flaps  Requests  Responses
                                00:00:00    0      10003    10003

RADIUS server: radius_server
Address: 4.1.1.2 Port: 1812
FPC/
PIC State      Duration      Previous
2/1 Active     00:54:45     Duration Flaps  Requests  Responses
                                00:00:00    0      10001    10001

```

**show unified-edge
ggsn-pgw aaa radius
statistics
dynamic-requests brief**

```
user@host> show unified-edge ggsn-pgw aaa radius statistics dynamic-requests brief
```

```

RADIUS client: rad1
Address: 7.1.1.2
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
RADIUS client: radius_server
Address: 4.1.1.2
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

```

**show unified-edge
ggsn-pgw aaa radius
statistics**

```

user@host> show unified-edge ggsn-pgw aaa radius statistics dynamic-requests detail
RADIUS client: rad1 (FPC/PIC: 2/1)
Address: 7.1.1.2

```

```
dynamic-requests detail
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
Forwarded: 0
Timeouts: 0
Delivered: 0
Invalid RADIUS codes: 0
Errors during processing: 0
Invalid RADIUS authenticators: 0
Invalid or missing Charging Ids: 0
Session mapping errors: 0
Time since counters were last cleared: 00:00:00
```

```
RADIUS client: radius_server (FPC/PIC: 2/1)
Address: 4.1.1.2
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
Forwarded: 0
Timeouts: 0
Delivered: 0
Invalid RADIUS codes: 0
Errors during processing: 0
Invalid RADIUS authenticators: 0
Invalid or missing Charging Ids: 0
Session mapping errors: 0
Time since counters were last cleared: 00:00:00
```

```
show unified-edge ggsn-pgw aaa radius statistics dynamic-requests summary
user@host> show unified-edge ggsn-pgw aaa radius statistics dynamic-requests summary

RADIUS client: rad1
Address: 7.1.1.2
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
RADIUS client: radius_server
Address: 4.1.1.2
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

show unified-edge ggsn-pgw aaa statistics

Syntax	show unified-edge ggsn-pgw aaa statistics (accounting authentication dynamic-requests) <brief detail extensive> <fpc-slot <i>fpc-slot</i> > <gateway-name <i>gateway-name</i> > <pic-slot <i>pic-slot</i> >
Release Information	Command introduced in Junos OS Mobility Release 11.2W. gateway-name option introduced in Junos OS Mobility Release 11.4W.
Description	Display the global statistics for accounting, authentication, and dynamic requests for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then statistics for all GGSNs and P-GWs are displayed.
Options	<p>authentication accounting dynamic-requests—Display the statistics for the specified parameter.</p> <p>brief detail extensive—(Optional) Display the specified level of output.</p> <p>fpc-slot <i>fpc-slot</i>—(Optional) Display the statistics for the specified Flexible PIC Concentrator (FPC).</p> <p>gateway-name <i>gateway-name</i>—(Optional) Display the statistics for the specified GGSN or P-GW.</p> <p>pic-slot <i>pic-slot</i>—(Optional) Display the statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear unified-edge ggsn-pgw aaa statistics on page 1019 • show unified-edge ggsn-pgw aaa radius statistics on page 1026
List of Sample Output	show unified-edge ggsn-pgw aaa statistics accounting brief on page 1038 show unified-edge ggsn-pgw aaa statistics accounting detail on page 1038 show unified-edge ggsn-pgw aaa statistics accounting extensive on page 1038 show unified-edge ggsn-pgw aaa statistics authentication brief on page 1038 show unified-edge ggsn-pgw aaa statistics authentication detail on page 1039 show unified-edge ggsn-pgw aaa statistics authentication extensive on page 1039 show unified-edge ggsn-pgw aaa statistics dynamic-requests brief on page 1039 show unified-edge ggsn-pgw aaa statistics dynamic-requests detail on page 1039 show unified-edge ggsn-pgw aaa statistics dynamic-requests extensive on page 1040
Output Fields	Table 60 on page 1036 lists the output fields for the show unified-edge ggsn-pgw aaa statistics command. Output fields are listed in the approximate order in which they appear.

Table 60: show unified-edge ggsn-pgw aaa statistics Output Fields

Field Name	Field Description	Level of Output
Gateway Name	Name of the GGSN or P-GW. If the statistics for all gateways are displayed, then "All" is displayed.	All levels
FPC/PIC	FPC and PIC slot numbers for which the statistics are displayed.	detail extensive
Accounting Module Statistics —The following statistics are displayed when the accounting option is used.		
Requests	Total number of Accounting Request packets sent.	All levels
Responses success	Number of Accounting Response Success packets received.	All levels
Requests timed out	Number of accounting requests that timed out and did not receive a response.	All levels
Requests retransmitted	Number of accounting requests that were retransmitted because they did not receive a response.	All levels
Transmit errors	Number of errors that occurred during the transmission of Accounting Request packets.	All levels
Response errors	Number of erroneous responses received.	All levels
Pending requests	Number of accounting requests waiting for responses.	All levels
Authentication Module Statistics —The following statistics are displayed when the authentication option is used.		
Requests	Number of access requests sent.	All levels
Accepts	Number of Access Accept responses received.	All levels
Rejects	Number of Access Reject responses received.	All levels
Challenges	Number of Access Challenge responses received.	All levels
Requests timed out	Number of authentication requests that did not receive a response.	All levels
Requests retransmitted	Number of authentication requests that were retransmitted because they did not receive a response.	All levels
Transmit errors	Number of errors that occurred during the transmission of Authentication Request packets.	All levels
Response errors	Number of erroneous responses received.	All levels
Pending requests	Number of authentication requests waiting for responses.	All levels

Table 60: show unified-edge ggsn-pgw aaa statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
Dynamic Requests Module Statistics —The following statistics are displayed when the dynamic-requests option is used.		
Requests received	Total number of dynamic requests received.	All levels
CoA requests received	Number of Change of Authorization (COA) requests received.	All levels
DM requests received	Number of Disconnect Message (DM) requests received.	All levels
CoA Acks sent	Number of COA acknowledgements sent.	All levels
CoA Nacks sent	Number of COA negative acknowledgements sent.	All levels
DM Acks sent	Number of Disconnect Message acknowledgements sent.	All levels
DM Nacks sent	Number of Disconnect Message negative acknowledgements sent.	All levels
Dropped	Number of dynamic authorization requests dropped.	All levels
Duplicates	Number of duplicate dynamic authorization requests.	detail extensive
Forwarded	Number of dynamic authorization requests that were forwarded.	detail extensive
Timeouts	Number of dynamic authorization requests that timed out.	detail extensive
Delivered	Number of dynamic authorization requests that were delivered.	extensive
Errors during processing	Number of dynamic authorization requests that could not be processed due to errors.	extensive
Unknown clients	Number of dynamic authorization requests that came from unknown clients.	extensive
Invalid AAA codes	Number of dynamic authorization requests with invalid AAA codes.	extensive
Invalid AAA authenticators	Number of dynamic authorization requests with invalid AAA authenticators.	extensive
Invalid or missing Charging Ids	Number of dynamic authorization requests with invalid charging IDs or that did not contain charging IDs.	extensive

Table 60: show unified-edge ggsn-pgw aaa statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
Session mapping errors	Number of dynamic authorization requests that caused session mapping errors during processing.	extensive
Invalid transactions ids	Number of dynamic authorization requests with invalid transaction IDs.	extensive

Sample Output

```
show unified-edge ggsn-pgw aaa statistics accounting brief
user@host> show unified-edge ggsn-pgw aaa statistics accounting brief
```

```
Accounting module statistics
Gateway Name: -A11-
Requests: 10001
Responses success: 10001
Requests timed out: 0
Requests retransmitted: 0
Transmit errors: 0
Response errors: 0
Pending requests: 0
```

```
show unified-edge ggsn-pgw aaa statistics accounting detail
user@host> show unified-edge ggsn-pgw aaa statistics accounting detail
```

The output for the **show unified-edge ggsn-pgw aaa statistics accounting** is the same for both the **detail** and **extensive** options.

```
show unified-edge ggsn-pgw aaa statistics accounting extensive
user@host> show unified-edge ggsn-pgw aaa statistics accounting extensive
```

```
Accounting module statistics (FPC/PIC: -A11-)
Gateway Name: 2/1
Requests: 10001
Responses success: 10001
Requests timed out: 0
Requests retransmitted: 0
Transmit errors: 0
Response errors: 0
Pending requests: 0
```

```
show unified-edge ggsn-pgw aaa statistics authentication brief
user@host> show unified-edge ggsn-pgw aaa statistics authentication brief
```

```
Authentication module statistics
Gateway Name: -A11-
Requests: 20004
Accepts: 20004
Rejects: 0
Challenges: 0
Requests timed out: 0
Requests retransmitted: 1812
Transmit errors: 0
Response errors: 0
```

Pending requests: 0

```

show unified-edge user@host> show unified-edge ggsn-pgw aaa statistics authentication detail
  ggsn-pgw aaa
  statistics
authentication detail
Authentication module statistics (FPC/PIC: -A11-)
Gateway Name: 2/1
Requests: 20004
Accepts: 20004
Rejects: 0
Challenges: 0
Requests timed out: 0
Requests retransmitted: 1812
Transmit errors: 0
Response errors: 0
Pending requests: 0

show unified-edge user@host> show unified-edge ggsn-pgw aaa statistics authentication extensive
  ggsn-pgw aaa
  statistics
authentication
  extensive
Authentication module statistics (FPC/PIC: -A11-)
Gateway Name: 2/1
Requests: 20004
Accepts: 20004
Rejects: 0
Challenges: 0
Requests timed out: 0
Requests retransmitted: 1812
Transmit errors: 0
Response errors: 0
Pending requests: 0

show unified-edge user@host> show unified-edge ggsn-pgw aaa statistics dynamic-requests brief
  ggsn-pgw aaa
  statistics
dynamic-requests brief
Dynamic requests module statistics
Gateway Name: -A11-
Requests received: 0
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

show unified-edge user@host> show unified-edge ggsn-pgw aaa statistics dynamic-requests detail
  ggsn-pgw aaa
  statistics
dynamic-requests
  detail
Dynamic requests module statistics (FPC/PIC: -A11-)
Gateway Name: 2/1
Requests received: 0
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

```

Forwarded: 0
Timeouts: 0

```
show unified-edge user@host> show unified-edge ggsn-pgw aaa statistics dynamic-requests extensive
  ggsn-pgw aaa      Dynamic requests module statistics (FPC/PIC: -All-)
  statistics        Gateway Name: 2/1
  dynamic-requests  Requests received: 0
  extensive         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
                   Forwarded: 0
                   Timeouts: 0
                   Delivered: 0
                   Errors during processing: 0
                   Unknown clients : 0
                   Invalid RADIUS codes: 0
                   Invalid RADIUS authenticators: 0
                   Invalid or missing Charging Ids: 0
                   Session mapping errors: 0
                   Invalid transactions ids: 0
```

show unified-edge ggsn-pgw address-assignment group

Syntax	<pre>show unified-edge ggsn-pgw address-assignment group <brief detail> <fpc-slot slot-number> <gateway gateway-name> <name group-name> <pic-slot slot-number> <routing-instance routing-instance-name></pre>
Release Information	<p>Command introduced in Junos OS Mobility Release 11.2W.</p> <p>gateway option introduced in Junos OS Mobility Release 11.4W.</p>
Description	Display the information for the mobile pool groups for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then information for all GGSNs and P-GWs is displayed.
Options	<p>none—(Same as brief) Display the information about the mobile pool groups in brief.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>fpc-slot fpc-slot pic-slot pic-slot—(Optional) Display the mobile pool groups for the services PIC in the specified FPC and PIC slots.</p> <p>gateway gateway-name—(Optional) Display the information about the mobile pool groups for the specified GGSN or P-GW.</p> <p>name name—(Optional) Display the information for the specified mobile pool group.</p> <p>routing-instance routing-instance—(Optional) Display the mobile pool group information for the specified routing instance.</p>
Required Privilege Level	<p>access—To view this statement in the configuration.</p> <p>access-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • show unified-edge ggsn-pgw address-assignment pool on page 1044
Output Fields	<p>Table 61 on page 1041 lists the output fields for the show unified-edge ggsn-pgw address-assignment group command. Output fields are listed in the approximate order in which they appear.</p>

Table 61: show unified-edge ggsn-pgw address-assignment-group Output Fields

Field Name	Field Description	Level of Output
Group	Name of the mobile pool group.	All levels
FPC/PIC	FPC and PIC slot numbers.	detail
Total addresses	Total number of addresses available in the mobile pool group.	All levels

Table 61: show unified-edge ggsn-pgw address-assignment-group Output Fields (*continued*)

Field Name	Field Description	Level of Output
Addresses in use	Number of addresses in the mobile pool group that are currently in use.	All levels
Address usage (percent)	Percentage utilization of the total addresses in the mobile pool group.	All levels
Routing instance	Routing instance to which the mobile pool group belongs.	All levels
Gateway	Gateway to which the PIC belongs.	detail
Pool information	<p>The following information about the mobile pools belonging to this mobile pool group is displayed:</p> <ul style="list-style-type: none"> • Name—Name of the mobile pool. • Total—Total number of addresses in the mobile pool. • In use—Number of addresses in the mobile pool that are in use. • Util (%)—Percentage of addresses in the mobile pool that have been used. 	All levels

Sample Output

```

show unified-edge ggsn-pgw address-assignment group brief
user@host> show unified-edge ggsn-pgw address-assignment group brief

Group: grp1
  Total addresses:      512
  Addresses in use:     301
  Address usage (percent): 59
  Routing instance:     default
  Pool information:

      Name                Total      In-use      Util
      pool2               256       254        99
      pool3               256        47         18

```

```

show unified-edge ggsn-pgw address-assignment group detail
user@host> show unified-edge ggsn-pgw address-assignment group detail

Group: grp1 (FPC/PIC: 4/0)
  Total addresses:      512
  Addresses in use:     0
  Address usage (percent): 0
  Routing instance:     default
  Gateway:              PGW
  Pool information:

      Name                Total      In-use      Util
      pool2               256        0          0
      pool3               256        0          0

```


Group: grp1 (FPC/PIC: 4/1)
Total addresses: 512
Addresses in use: 301
Address usage (percent): 59
Routing instance: default
Gateway: PGW
Pool information:

Name	Total	In-use	Util (%)
pool2	256	254	99
pool3	256	47	18

show unified-edge ggsn-pgw address-assignment pool

Syntax `show unified-edge ggsn-pgw address-assignment pool`
 `<brief | detail | summary>`
 `<fpc-slot fpc-slot>`
 `<gateway gateway-name>`
 `<name pool-name>`
 `<pic-slot pic-slot>`
 `<range range-name>`
 `<ranges>`
 `<routing-instance routing-instance>`

Release Information Command introduced in Junos OS Mobility Release 11.2W.
 gateway option introduced in Junos OS Mobility Release 11.4W.

Description Display the information about the mobile pools for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then information for all GGSNs and P-GWs is displayed

Options **none**—(Same as brief) Display the address information about the mobile pools in brief.

brief | detail | summary—(Optional) Display the specified level of output.

fpc-slot fpc-slot pic-slot pic-slot—(Optional) Display the mobile pool information for the services PIC in the specified FPC and PIC slots.

gateway gateway-name—(Optional) Display the mobile pool information for the specified GGSN or P-GW.

name name—(Optional) Display the information for the specified mobile pool.



NOTE: Specifying the mobile pool is mandatory if you use either the **range range-name** or the **ranges** option.

range range-name—Display the information for the specified range in the specified pool.

ranges—Display the information for all the ranges in the specified pool.

routing-instance routing-instance—(Optional) Display the mobile pool information for the specified routing instance.

Required Privilege Level view

Related Documentation • [clear unified-edge ggsn-pgw address-assignment pool on page 1020](#)

Output Fields Table 62 on page 1045 lists the output fields for the **show unified-edge ggsn-pgw address-assignment pool** command. Output fields are listed in the approximate order in which they appear.

Table 62: show unified-edge ggsn-pgw address-assignment pool Output Fields

Field Name	Field Description	Level of Output
Pool or Name	Name of the mobile pool.	All levels
FPC/PIC	FPC and PIC slots of the services PIC for which the mobile pool information is displayed.	detail
Total Addresses or Total	Total number of addresses available in the mobile pool.	All levels
Addresses in use or In Use	Number of addresses that have been allocated.	All levels
Addresses skipped	Number of addresses that are excluded from allocation.	brief detail
Address usage (percent) or Util (%)	Percentage of the total addresses used.	All levels
Addresses in aging period	Number of addresses that are currently being released and that cannot be allocated.	brief detail
Routing Instance	Name of the routing instance to which the mobile pool belongs.	All levels
Gateway	Gateway to which the services PIC belongs.	detail
Pool Maintenance Mode	Service mode of the mobile pool; for example, operational or maintenance.	detail
Address chunks	Number of chunks of IP addresses in the mobile pool (for the services PIC) that are currently being assigned	detail
Total address chunk size	Total number of addresses in the address chunk (for the services PIC).	detail
Total allocation failures	Total number of addresses that could not be allocated.	detail

Sample Output

```
show unified-edge ggsn-pgw user@host> show unified-edge ggsn-pgw address-assignment pool brief
```

```
address-assignment Pool: pool1
pool brief      Total addresses:      16777215
                Addresses in use:      1600
                Addresses skipped:      416
                Address usage (percent): 0.
                Addresses in aging period: 1600
                Routing instance:      default
```

```
Pool: pool2
  Total addresses:      256
  Addresses in use:      254
  Addresses skipped:      2
  Address usage (percent): 99
  Addresses in aging period: 0
  Routing instance:      default
```

```
[...output truncated...]
```

```
show unified-edge user@host> show unified-edge ggsn-pgw address-assignment pool detail
ggsn-pgw
address-assignment
pool detail
```

```
Pool: pool1 (FPC/PIC: 4/0)
  Pool Maintenance Mode: Operational
  Total addresses:      16777215
  Addresses in use:      822
  Addresses skipped:      208
  Address usage (percent): 0.
  Addresses in aging period: 822
  Routing instance:      default
  Gateway:              PGW
  Address chunks:        26
  Total address chunk size: 26416
  Total allocation failures: 0
```

```
Pool: pool1 (FPC/PIC: 4/1)
  Pool Maintenance Mode: Operational
  Total addresses:      16777215
  Addresses in use:      778
  Addresses skipped:      208
  Address usage (percent): 0.
  Addresses in aging period: 778
  Routing instance:      default
  Gateway:              PGW
  Address chunks:        26
  Total address chunk size: 26416
  Total allocation failures: 0
```

```
Pool: pool2 (FPC/PIC: 4/0)
  Pool Maintenance Mode: Operational
  Total addresses:      256
  Addresses in use:      0
  Addresses skipped:      0
  Address usage (percent): 0
  Addresses in aging period: 0
  Routing instance:      default
  Gateway:              PGW
  Address chunks:        0
  Total address chunk size: 0
  Total allocation failures: 0
```

[...output truncated...]

```

show unified-edge user@host> show unified-edge ggsn-pgw address-assignment pool summary
ggsn-pgw
address-assignment
pool summary

```

Name	Total	In-use	Util (%)	Routing instance
pool1	16777215	1600	0.	default
pool2	256	254	99	default
pool3	256	47	18	default
v4_pool	16777216	0	0	default
v4_pool1	16777215	0	0	default
v6_pool	16777215	0	0	default
v6_pool1	16777215	0	0	default

show unified-edge ggsn-pgw address-assignment service-mode

Syntax	<code>show unified-edge ggsn-pgw address-assignment service-mode</code> <code><brief detail></code> <code><pool <i>pool-name</i>></code> <code><routing-instance <i>routing-instance-name</i>></code>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Display service mode information about mobile pools.
Options	<p>none—Display the service mode information in brief.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>pool <i>pool-name</i>—(Optional) Display the service mode information for the specified mobile pool.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Display the service mode information about the mobile pools that are part of the specified routing instance.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Example: Changing Mobility Pool Attributes on page 416
List of Sample Output	show unified-edge ggsn-pgw address-assignment service-mode brief on page 1049 show unified-edge ggsn-pgw address-assignment service-mode detail on page 1049
Output Fields	Table 63 on page 1048 lists the output fields for the <code>show unified-edge ggsn-pgw address-assignment service-mode</code> command. Output fields are listed in the approximate order in which they appear.

Table 63: show unified-edge ggsn-pgw address-assignment service-mode Output Fields

Field Name	Field Description
Pool Name	Name of the mobile pool.
Routing Instance	Routing instance to which the mobile pool belongs.
Service Mode	Service mode for the mobile pool: <ul style="list-style-type: none"> • Operational—Mobile pool is in operational mode. • Maintenance—Mobile pool is in maintenance mode. • Maintenance - Active Phase—All the attributes of the mobile pool can be modified. • Maintenance - In/Out Phase—Only the non-maintenance mode attributes of the mobile pool can be modified.

Sample Output

```

show unified-edge user@host> show unified-edge ggsn-pgw address-assignment service-mode brief
  ggsn-pgw
address-assignment
service-mode brief
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.

```

Routing-Instance	Pool Name	Service Mode
default	my_pool	Operational
default	v6_pool	Operational

```

show unified-edge user@host> show unified-edge ggsn-pgw address-assignment service-mode detail
  ggsn-pgw
address-assignment
service-mode detail
Routing Instance: default
Pool Name       : my_pool
Service Mode    : Operational

Routing Instance: default
Pool Name       : v6_pool
Service Mode    : Operational

```

show unified-edge ggsn-pgw address-assignment statistics

Syntax	<pre>show unified-edge ggsn-pgw address-assignment statistics <brief detail> <fpc-slot fpc-slot> <gateway gateway-name> <pic-slot pic-slot></pre>
Release Information	<p>Command introduced in Junos OS Mobility Release 11.2W.</p> <p>gateway option introduced in Junos OS Mobility Release 11.4W.</p>
Description	Display the address assignment statistics for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then the consolidated statistics for all GGSNs and P-GWs are displayed.
Options	<p>none—(Same as brief) Display the address assignment statistics in brief.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>fpc-slot fpc-slot pic-slot pic-slot—(Optional) Display the statistics for the services PIC in the specified FPC and PIC slots.</p> <p>gateway gateway-name—(Optional) Display the consolidated statistics for the specified GGSN or P-GW.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear unified-edge ggsn-pgw address-assignment statistics on page 1021
Output Fields	Table 64 on page 1050 lists the output fields for the show unified-edge ggsn-pgw address-assignment statistics command. Output fields are listed in the approximate order in which they appear.

Table 64: show unified-edge ggsn-pgw address-assignment statistics Output Fields

Field Name	Field Description	Level of Output
FPC/PIC	FPC and PIC slots for which the statistics are displayed.	detail
Gateway	Name of the GGSN or P-GW.	detail gateway
Total address allocations	Total number of addresses allocated.	All levels
Total allocation failures	Total number of address allocations that failed.	All levels
Total address releases	Total number of addresses that were released.	All levels

Sample Output

```
show unified-edge ggsn-pgw address-assignment statistics user@host> show unified-edge ggsn-pgw address-assignment statistics
Address assignment statistics
Total address allocations: 1101
Total allocation failures: 0
Total address releases: 800

show unified-edge ggsn-pgw address-assignment statistics detail user@host> show unified-edge ggsn-pgw address-assignment statistics detail
Address assignment statistics (FPC/PIC: 4/0)
Gateway: PGW
Total address allocations: 416
Total allocation failures: 0
Total address releases: 416

Address assignment statistics (FPC/PIC: 4/1)
Gateway: PGW
Total address allocations: 685
Total allocation failures: 0
Total address releases: 384
```


CHAPTER 30

Anchor Packet Forwarding Engine Redundancy and Aggregated Multiservices High Availability Operational Commands


request interface load-balancing revert (Aggregated Multiservices)

Syntax	<code>request interface load-balancing revert <i>interface-name</i></code>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Revert the aggregated multiservices member interface (mams-) from the inactive state to the active or backup state based on the configuration and the operational state of the aggregated multiservices interface.
Options	<i>interface-name</i> —Name of the member interface. The member interface format is mams-a/b/0 , where a is the FPC slot number and b is the PIC slot number.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• request interface load-balancing switchover (Aggregated Multiservices) on page 1055
List of Sample Output	request interface load-balancing revert mams-4/0/0 (Aggregated Multiservices) on page 1054
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

<code>request interface load-balancing revert mams-4/0/0 (Aggregated Multiservices)</code>	<code>user@host> request interface load-balancing revert mams-4/0/0 request succeeded</code>
--	---

request interface load-balancing switchover (Aggregated Multiservices)

Syntax	<code>request interface load-balancing switchover <i>interface-name</i> <force></code>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	<p>Switch the active member interface to the backup state.</p> <p>In the case of mobile control plane redundancy, the behavior depends on the replication state of the member interface:</p> <ul style="list-style-type: none"> • If the sync state is in-sync, then the active member is rebooted and the backup member becomes the new active member. • If the sync-state is in-progress, then the force option must be used to force the switchover. <div style="display: flex; align-items: center; margin-top: 10px;">  <div style="margin-left: 10px;"> <p>WARNING: In this case, there is a risk of losing subscriber information because the synchronization has not yet been completed.</p> </div> </div>
Options	<p><i>interface-name</i>—Name of the member interface. The member interface format is mams-a/b/0, where a is the FPC slot number and b is the PIC slot number.</p> <p>force—(Optional) Force the switchover from the active member to the backup member.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • request interface load-balancing revert (Aggregated Multiservices) on page 1054
List of Sample Output	request interface load-balancing switchover force mams-4/0/0 (Aggregated Multiservices) on page 1055
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

```

request interface user@host> request interface load-balancing switchover force mams-4/0/0
load-balancing    Switchover Initiated
switchover force
mams-4/0/0
(Aggregated
Multiservices)

```

show interfaces anchor-group (Aggregated Packet Forwarding Engine)

Syntax `show interfaces anchor-group`
`<brief | detail>`
`interface-name`

Release Information Command introduced in Junos OS Mobility Release 11.2W.

Description Display interface information for the aggregated Packet Forwarding Engine group.

Options **none**—(Same as brief) Display a summary of the aggregated Packet Forwarding Engine interface information.

brief | detail—(Optional) Display the specified level of output.

interface-name—Name of the interface within the anchor Packet Forwarding Engine group.



NOTE: The interface must be an aggregated Packet Forwarding Engine interface (apfe-).

Required Privilege Level view

Related Documentation • [show unified-edge ggsn-pgw system interfaces on page 1066](#)

List of Sample Output [show interfaces anchor-group brief on page 1057](#)
[show interfaces anchor-group detail on page 1058](#)

Output Fields [Table 65 on page 1056](#) lists the output fields for the `show interfaces anchor-group` command. Output fields are listed in the approximate order in which they appear.

Table 65: show interfaces anchor-group

Field Name	Field Description	Level of Output
Redundancy Status Legend	<p>Legend for the redundancy status.</p> <ul style="list-style-type: none"> • Active—Indicates that the anchor Packet Forwarding Engine is operational. • Inactive—Indicates that the anchor Packet Forwarding Engine is not operational. • PF—Indicates that the primary Packet Forwarding Engine anchor has failed. • WS—Indicates that the primary Packet Forwarding Engine is protected by a secondary Packet Forwarding Engine in warm standby mode. 	All levels
Group	Name of the aggregated Packet Forwarding Engine group.	brief none
Mode	Redundancy mode in which the aggregated Packet Forwarding Engine group operates. Currently, only warm standby mode is supported.	brief none

Table 65: show interfaces anchor-group (continued)

Field Name	Field Description	Level of Output
Sub-group ID	Redundancy subgroups within the anchor Packet Forwarding Engine group configuration that has FPCs as members. This is derived out of the Packet Forwarding Engines on a given FPC. For example, if the first Packet Forwarding Engine is assigned the number 0, then all the other Packet Forwarding Engines with sub-group ID 0 form the N:1 redundancy group.	brief none
Interface	Anchor Packet Forwarding Engine interface (pfe-).	brief detail none
Configured State	State in which the anchor Packet Forwarding Engine was configured. <ul style="list-style-type: none"> • Primary: Indicates that the anchor Packet Forwarding Engine is in the pool of primary members. • Secondary: Indicates that the anchor Packet Forwarding Engine is a backup to all the primary members. 	brief detail none
Operational State	Indicates whether the anchor Packet Forwarding Engine is operational (Active) or not operational (Inactive).	brief detail none
Redundancy State	Redundancy state (primary or secondary) in which the anchor Packet Forwarding Engine was configured.	brief detail none
Group Name	Name of the aggregated Packet Forwarding Engine group.	detail
Group Mode	Redundancy mode in which the aggregated Packet Forwarding Engine group operates. Currently, only warm standby mode is supported.	detail
Group Id	Internal ID generated for the group.	detail
Switchover information	Switchover details, if any.	detail
Subgroup identifier	Redundancy subgroups within the anchor Packet Forwarding Engine group configuration that has FPCs as members. This is derived out of the Packet Forwarding Engines on a given FPC. For example, if the first Packet Forwarding Engine is assigned the number 0, then all the other Packet Forwarding Engines with subgroup ID 0 form the N:1 redundancy group.	detail

Sample Output

```

show interfaces anchor-group brief
user@host> show interfaces anchor-group brief
Redundancy Status Legend:

Active: Operational      Inactive: Non-operational
MS: Manually switched    PF: Primary failed
HS: Hot standby          WS: Warm standby

Group   Mode   Sub-group   Interface   Configured   Operational   Redundancy
      ID                               State        State        State
-----
apfe0   WS     0           pfe-4/0/0   Primary     Active        Primary
          pfe-5/0/0   Secondary    Active        Secondary

```

2	pfe-4/2/0	Primary	Active	Primary
	pfe-5/2/0	Secondary	Active	Secondary

show interfaces
anchor-group detail

```
user@host> show interfaces anchor-group detail
Active: Operational           Inactive: Non-operational
MS: Manually switched        PF: Primary failed
HS: Hot standby              WS: Warm standby

Group Name: apfe0
Group Mode: WS                Group Id: 65
Switchover information: None
Interface pfe-4/2/0
  Configured state: Primary    Operational state: Active
  Redundancy state: Primary
  Subgroup identifier: 2
Interface pfe-4/0/0
  Configured state: Primary    Operational state: Active
  Redundancy state: Primary
  Subgroup identifier: 0
Interface pfe-5/0/0
  Configured state: Secondary   Operational state: Active
  Redundancy state: Secondary
  Subgroup identifier: 0
Interface pfe-5/2/0
  Configured state: Secondary   Operational state: Active
  Redundancy state: Secondary
  Subgroup identifier: 2
```


show interfaces load-balancing (Aggregated Multiservices)

Syntax	show interfaces load-balancing <detail> <interface-name>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Display information about the aggregated multiservices interface (ams) as well as its individual member interfaces and the status of the replication state.
Options	<p>none—Display a summary of the aggregated multiservices interface information.</p> <p>detail—(Optional) Display the specified level of output.</p> <p>interface-name—(Optional) Name of the aggregated multiservices interface (ams). If this is omitted, then the information for all the aggregated multiservices interfaces, including those used in control plane redundancy and high availability (HA) for service applications, is displayed.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show unified-edge ggsn-pgw system interfaces on page 1066
List of Sample Output	show interfaces load-balancing on page 1060 show interfaces load-balancing detail on page 1060 show interfaces load-balancing ams0 detail on page 1061
Output Fields	Table 66 on page 1059 lists the output fields for the show interfaces load-balancing command. Output fields are listed in the approximate order in which they appear.

Table 66: show interfaces load-balancing Output Fields

Field Name	Field Description	Level of Output
Interface	Aggregated multiservices interface (ams).	detail none
State	<p>State of the aggregated multiservices interface. The following states are possible:</p> <ul style="list-style-type: none"> • Wait for Members—None of the member interfaces are powered on yet. • Members Seen—All of the member interfaces are online. • Wait Timer—At least one of the member interfaces has joined the ams interface. • Up—The ams interface is up with the current joined member interfaces. 	detail none
Last change	Time (in <i>hh:mm:ss [hours:minutes:seconds]</i> format) when the state last changed.	detail none
Members	Number of member interfaces (mams-).	none

Table 66: show interfaces load-balancing Output Fields (*continued*)

Field Name	Field Description	Level of Output
Member count	Number of member interfaces (mams-).	detail
HA Model	High availability (HA) model supported on the interface.	detail none
Members	<p>The following information about the member interfaces is displayed:</p> <ul style="list-style-type: none"> • Interface—Name of the member interface. • Weight—This output can be ignored for the current release. • State—Indicates the state of the member interface (mams-). The following states are possible: <ul style="list-style-type: none"> • Active—The member is an active member. • Backup—The member is a backup. • Discard—The member has not yet rejoined the ams interface after failure. • Down—The member has not yet powered on. • Inactive—The member has failed to rejoin the ams interface within the configured rejoin-timeout. • Invalid—The Multiservices PIC corresponding to the member interface has been configured but is not physically present in the chassis. 	detail
Sync-state	<p>Synchronization (sync) status of the control plane redundancy. The sync state is displayed only when the ams interface is Up.</p> <ul style="list-style-type: none"> • Interface—Name of the member interface. • Status—The synchronization status of the member interfaces. <ul style="list-style-type: none"> • In progress—The active member is currently synchronizing its state information with the backup member. • In sync—The active member has finished synchronizing its state information with the backup and the backup is ready to take over if the active member fails. • NA (Not applicable)—The backup member is not yet ready to synchronize with the active (primary) member. This may occur if the backup is still powered off or still booting. • Unknown—The daemons are still initializing and the state information is unavailable. 	detail

Sample Output

```

show interfaces user@host> show interfaces load-balancing
load-balancing Interface State      Last change  Members  HA Model
                  ams0      Up           00:10:02    4        Many-to-One

```

```

show interfaces user@host> show interfaces load-balancing detail
load-balancing detail Load-balancing interfaces detail
Interface           : ams0
State                : Up
Last change         : 00:10:23
Member count        : 4
HA Model            : Many-to-One
Members              :

```

Interface	Weight	State
mams-4/0/0	10	Active
mams-4/1/0	10	Active
mams-5/0/0	10	Active
mams-5/1/0	10	Backup

Sync-state :

Interface	Status
mams-4/0/0	Unknown
mams-4/1/0	Unknown
mams-5/0/0	Unknown

```

show interfaces load-balancing ams0 detail
user@host> show interfaces load-balancing ams0 detail
Load-balancing interfaces detail
Interface      : ams0
State          : Up
Last change    : 00:11:28
Member count   : 4
HA Model       : Many-to-One
Members        :
  Interface    Weight  State
  mams-4/0/0   10     Active
  mams-4/1/0   10     Active
  mams-5/0/0   10     Active
  mams-5/1/0   10     Backup
Sync-state     :
  Interface    Status
  mams-4/0/0   Unknown
  mams-4/1/0   Unknown
  mams-5/0/0   Unknown

```

show services ipsec-vpn ipsec security-associations

Syntax	show services ipsec-vpn ipsec security-associations <brief detail extensive> <service-set service-set-name>
Release Information	Command introduced before Junos OS Release 7.4.
Description	(Adaptive services interface only) Display IPsec security associations for the specified service set. If no service set is specified, the security associations for all service sets are displayed.
Options	<p>none—Display standard information about IPsec security associations for all service sets.</p> <p>brief detail extensive—(Optional) Display the specified level of output.</p> <p>service-set service-set-name—(Optional) Display information about a particular service set.</p>
Required Privilege Level	view
List of Sample Output	show services ipsec-vpn ipsec security associations detail on page 1064 show services ipsec-vpn ipsec security associations extensive on page 1064
Output Fields	Table 67 on page 1062 lists the output fields for the show services ipsec-vpn ipsec security-associations command. Output fields are listed in the approximate order in which they appear.

Table 67: show services ipsec-vpn ipsec security-associations Output Fields

Field Name	Field Description	Level of Output
Service set	Name of the service set for which the IPsec security associations are defined. If appropriate, includes the outside service interface VRF name.	All levels
Rule	Name of the rule set applied to the security association.	detail extensive
Term	Name of the IPsec term applied to the security association.	detail extensive
Tunnel index	Numeric identifier of the specific IPsec tunnel for the security association.	detail extensive
Anchored PIC	Services PIC on which the IPsec tunnel is anchored. This field is displayed only if the service set is applied over an AMS interface; for example ams0 .	detail extensive
Local gateway	Gateway address of the local system.	All levels
Remote gateway	Gateway address of the remote system.	All levels
IPsec inside interface	Name of the logical interface hosting the IPsec tunnels.	All levels

Table 67: show services ipsec-vpn ipsec security-associations Output Fields (*continued*)

Field Name	Field Description	Level of Output
Local identity	Prefix and port number of the local end.	All levels
Remote identity	Prefix and port number of the remote end.	All levels
Primary remote gateway	IP address of the configured primary remote peer.	All levels
Backup remote gateway	IP address of the configured backup remote peer.	All levels
State	State of the primary or backup interface: Active , Offline , or Standby . Both ES PICs are initialized to Offline . For primary and backup peers, State can be Active or Standby . If both peers are in a state of Standby , no connection exists yet between the two peers.	All levels
Failover counter	Number of times a PIC switched between the primary and backup interfaces, or the number of times the tunnel switched between the primary and remote peers since the software was activated.	All levels
Direction	Direction of the security association: inbound or outbound .	All levels
SPI	Value of the security parameter index.	All levels
AUX-SPI	Value of the auxiliary security parameter index: <ul style="list-style-type: none"> When the value of Protocol is AH or ESP, AUX-SPI is always 0. When the value of Protocol is AH+ESP, AUX-SPI is always a positive integer. 	All levels
Mode	Mode of the security association: <ul style="list-style-type: none"> transport—Protects single host-to-host protections. tunnel—Protects connections between security gateways. 	detail extensive
Type	Type of security association: <ul style="list-style-type: none"> manual—Security parameters require no negotiation. They are static, and are configured by the user. dynamic—Security parameters are negotiated by the IKE protocol. Dynamic security associations are not supported in transport mode. 	detail extensive
State	Status of the security association: <ul style="list-style-type: none"> Installed—The security association is installed in the security association database. (For transport mode security associations, the value of State must always be Installed.) Not installed—The security association is not installed in the security association database. 	detail extensive

Table 67: show services ipsec-vpn ipsec security-associations Output Fields (*continued*)

Field Name	Field Description	Level of Output
Protocol	Protocol supported: <ul style="list-style-type: none"> transport mode supports Encapsulation Security Protocol (ESP) or Authentication Header (AH). tunnel mode supports ESP or AH+ESP. 	All levels
Authentication	Type of authentication used: hmac-md5-96 , hmac-sha1-96 , or none .	detail extensive
Encryption	Type of encryption algorithm used: aes-cbc (128 bits) , aes-cbc (192 bits) , aes-cbc (256 bits) , des-cbc , 3des-cbc , or None .	detail
Soft lifetime Hard lifetime	Each lifetime of a security association (SA) has two display options, hard and soft, one of which must be present for a dynamic security association. The hard lifetime specifies the lifetime of the SA. The soft lifetime, which is derived from the hard lifetime, informs the IPsec key management system that the SA is about to expire. This information allows the key management system to negotiate a new SA before the hard lifetime expires. <ul style="list-style-type: none"> Expires in seconds seconds—Number of seconds left until the security association expires. Expires in kilobytes kilobytes—Number of kilobytes left until the security association expires. 	detail extensive
Anti-replay service	State of the service that prevents packets from being replayed: Enabled or Disabled .	detail extensive
Replay window size	Configured size, in packets, of the antireplay service window: 32 or 64 . The antireplay window size protects the receiver against replay attacks by rejecting old or duplicate packets. If the replay window size is 0 , antireplay service is disabled.	detail

Sample Output

```

show services ipsec-vpn ipsec security associations detail
user@host> show services ipsec-vpn ipsec security-associations detail
Service set: huffer, IKE Routing-instance: default

Rule: _junos_, Term: tunnel1, Tunnel index: 1, Anchored pic: mams-5/1/0
Local gateway: 4.1.1.2, Remote gateway: 4.1.1.1
IPSec inside interface: ams0.1, Tunnel MTU: 1500
Local identity: ipv4(any:0,[0..3]=4.1.1.2)
Remote identity: ipv4(any:0,[0..3]=4.1.1.1)

show services ipsec-vpn ipsec security associations extensive
user@host> show services ipsec-vpn ipsec security-associations extensive
Service set: snart, IKE Routing-instance: default

Rule: _junos_, Term: tunnel1, Tunnel index: 1, Anchored pic: mams-5/1/0
Local gateway: 3.1.100.101, Remote gateway: 3.1.100.2
IPSec inside interface: ams0.1, Tunnel MTU: 1500
Local identity: ipv4(any:0,[0..3]=5.1.0.2)
Remote identity: ipv4(any:0,[0..3]=4.1.0.2)

```

Direction: inbound, SPI: 2417504417, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 28704 seconds
Hard lifetime: Expires in 28794 seconds
Anti-replay service: Enabled, Replay window size: 128

Direction: outbound, SPI: 4201112312, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 28704 seconds
Hard lifetime: Expires in 28794 seconds
Anti-replay service: Enabled, Replay window size: 128

show unified-edge ggsn-pgw system interfaces

Syntax	show unified-edge ggsn-pgw system interfaces <gateway gateway>
Release Information	Command introduced in Junos OS Mobility Release 11.2W. gateway option introduced in Junos OS Mobility Release 11.4W.
Description	Display information about the aggregated Packet Forwarding Engine and the aggregated multiservices (AMS) interfaces and their states on one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then information for all GGSNs and P-GWs is displayed.
Options	none —Display information for one or more GGSNs and P-GWs. gateway gateway-name —(Optional) Display information for the specified gateway.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show interfaces anchor-group (Aggregated Packet Forwarding Engine) on page 1056 • show interfaces load-balancing (Aggregated Multiservices) on page 1059 • show unified-edge ggsn-pgw resource-manager clients on page 1280
List of Sample Output	show unified-edge ggsn-pgw system interfaces on page 1067
Output Fields	Table 68 on page 1066 lists the output fields for the show unified-edge ggsn-pgw system interfaces command. Output fields are listed in the approximate order in which they appear.

Table 68: show unified-edge ggsn-pgw system interfaces

Field Name	Field Description
Gateway	Name of the GGSN or P-GW.
Interfaces	Name of the interface: <ul style="list-style-type: none"> • Aggregated multiservices; for example, ams0 • Aggregated Packet Forwarding Engine; for example, apfe1 • Member of aggregated multiservices; for example, mams-1/0/0 • Multiservices; for example, ms-1/0/0 • Packet Forwarding Engine; for example, pfe-0/1/0
Members	For ams and apfe interfaces, the member interfaces that are part of the aggregated interfaces are displayed.
Operational State	Indicates whether the interface is operational (Active) or not (Inactive).

Table 68: show unified-edge ggsn-pgw system interfaces (*continued*)

Field Name	Field Description
Redundancy Role	Redundancy state in which the interface is configured: <ul style="list-style-type: none"> • Primary—The interface is a primary member. • Secondary—The interface is a backup to all the primary members. • Standalone—The interface has not been configured for redundancy.

Sample Output

```

show unified-edge user@host> show unified-edge ggsn-pgw system interfaces
ggsn-pgw system  Gateway: PGW
interfaces
      Interfaces      Members      Operational      Redundancy
                  State
ms-1/0/0            Active      Standalone
ms-1/1/0            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

```

show unified-edge sgw system interfaces

Syntax	show unified-edge sgw system interfaces <gateway gateway>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Display information about the aggregated Packet Forwarding Engine and the aggregated multiservices (AMS) interfaces and their states on one or more configured Serving Gateways (S-GWs). If a gateway is not specified, then information for all configured S-GWs is displayed.
Options	gateway gateway —(Optional) Display interface information for the specified gateway.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show interfaces anchor-group (Aggregated Packet Forwarding Engine) on page 1056 • show interfaces load-balancing (Aggregated Multiservices) on page 1059 • show unified-edge sgw resource-manager clients on page 1290
List of Sample Output	show unified-edge sgw system interfaces on page 1069
Output Fields	Table 69 on page 1068 lists the output fields for the show unified-edge sgw system interfaces command. Output fields are listed in the approximate order in which they appear.

Table 69: show unified-edge sgw system interfaces Output Fields

Field Name	Field Description
Gateway	Name of the S-GW.
Interfaces	Name of the interface: <ul style="list-style-type: none"> • Aggregated multiservices; for example, ams0 • Aggregated Packet Forwarding Engine, for example, apfe1 • Member of aggregated multiservices; for example mams-1/0/0 • Multiservices; for example, ms-3/0/0 • Packet Forwarding Engine; for example pfe-4/2/0
Members	For ams and apfe interfaces, the member interfaces that are part of the aggregated interfaces are displayed.
Operational State	Indicates whether the interface is operational (Active) or not (Inactive).

Table 69: show unified-edge sgw system interfaces Output Fields (*continued*)

Field Name	Field Description
Redundancy Role	<p>Redundancy state in which the interface is configured:</p> <ul style="list-style-type: none"> • Primary—The interface is a primary member. • Secondary—The interface is a backup to all the primary members. • Standalone—The interface is not configured for redundancy.

Sample Output

```

show unified-edge sgw system interfaces user@host> show unified-edge sgw system interfaces
Gateway: SGW
  Interfaces      Members      Operational State      Redundancy Role
ms-3/0/0          Active       Standalone
ms-3/1/0          Inactive     Standalone
pfe-4/0/0         Active       Standalone
pfe-4/2/0         Active       Standalone

```


CHAPTER 31

APN and Related Operational Commands

show services hcm statistics

Syntax `show services hcm statistics`
`<rule rule-name>`

Release Information Command introduced in Junos OS Mobility Release 11.4W.

Description Display the statistics collected for HTTP header enrichment for a specified tag rule.



NOTE: This command displays an output only if the count statement (at the [edit services hcm tag-rule *rule-name* term *term-name* then] hierarchy level) is configured for the term in a tag rule.

Options **none**—Currently, no statistics are displayed when this command is run without a tag rule specified.

rule rule-name—Display the statistics for the specified tag rule.

Required Privilege Level view

Related Documentation

- [count \(HTTP Header Enrichment\) on page 694](#)
- [Example: Configuring HTTP Header Enrichment on page 138](#)

List of Sample Output [show services hcm statistics rule rule1 on page 1072](#)

Output Fields [Table 70 on page 1072](#) lists the output fields for the `show services hcm statistics` command. Output fields are listed in the approximate order in which they appear.

Table 70: show services hcm statistics Output Fields

Field Name	Field Description
Interface	Name of the interface for which the statistics are displayed.
Term ID	Identifier for the term (in the tag rule) for which the statistics are displayed.
Hits	Number of times that the term was matched. This field displays the aggregate number of hits on service sets that include the term.

Sample Output

```
show services hcm statistics rule rule1
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

clear unified-edge ggsn-pgw statistics

Syntax	<code>clear unified-edge ggsn-pgw statistics gateway <i>gateway</i></code> <code><apn <i>apn</i>></code>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Clear the statistics for the specified gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW).
Options	gateway <i>gateway</i> —Clear the statistics for the specified GGSN or P-GW. apn <i>apn</i> —(Optional) Clear the statistics for the specified access point name (APN).
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show unified-edge ggsn-pgw statistics on page 1088
List of Sample Output	clear unified-edge ggsn-pgw statistics gateway pgw on page 1074
Output Fields	No message is displayed on successful execution of this command; otherwise an error message is displayed.

Sample Output

<code>clear unified-edge ggsn-pgw statistics gateway pgw</code>	<code>user@host> clear unified-edge ggsn-pgw statistics gateway pgw</code>
---	---


clear unified-edge ggsn-pgw subscribers

Syntax	<pre>clear unified-edge ggsn-pgw subscribers gateway <i>gateway</i> <apn <i>apn</i>> <imsi <i>imsi</i>> <msisdn <i>msisdn</i>> <routing-instance <i>routing-instance</i>> <v4-addr <i>v4-addr</i>> <v6-addr <i>v6-addr</i>></pre>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Clear the subscribers on the specified gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW).
Options	<p>gateway <i>gateway</i>—Clear the subscribers for the GGSN or P-GW.</p> <p>apn <i>apn</i>—(Optional) Clear the subscribers for the specified APN.</p> <p>imsi <i>imsi</i>—(Optional) Clear the subscriber matching the specified International Mobile Subscriber Identity (IMSI).</p> <p>msisdn <i>msisdn</i>—(Optional) Clear the subscriber matching the specified Mobile Station ISDN (MSISDN) number.</p> <p>routing-instance <i>routing-instance</i>—(Optional) Clear the subscriber information for the specified routing instance.</p> <p>v4-addr <i>v4-addr</i>—(Optional) Clear the subscriber information for the specified IPv4 address of the subscriber's user equipment (UE).</p> <p>v6-addr <i>v6-addr</i>—(Optional) Clear the subscriber information for the specified IPv6 address of the subscriber's user equipment.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • clear unified-edge ggsn-pgw subscribers charging on page 1077 • clear unified-edge ggsn-pgw subscribers peer on page 1078 • show unified-edge ggsn-pgw subscribers on page 1095
List of Sample Output	clear unified-edge ggsn-pgw subscribers gateway pgw on page 1076
Output Fields	No message is displayed on successful execution of this command; otherwise an error message is displayed.

Sample Output

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

clear unified-edge ggsn-pgw subscribers charging

Syntax	<code>clear unified-edge ggsn-pgw subscribers charging gateway <i>gateway</i></code> <code><charging-profile <i>charging-profile</i>></code> <code><transport-profile <i>transport-profile</i>></code>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Clear the charging information for subscribers on the specified gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW).
Options	<p>gateway <i>gateway</i>—Clear the charging information for all subscribers for the specified GGSN or P-GW.</p> <p>charging-profile <i>charging-profile</i>—(Optional) Clear the subscriber matching the specified charging profile name.</p> <p>transport-profile <i>transport-profile</i>—(Optional) Clear the subscriber matching the specified transport profile name.</p>
<div>  <p>NOTE: You must specify either a charging profile or a transport profile to run this command.</p> </div>	
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • clear unified-edge ggsn-pgw subscribers on page 1075 • clear unified-edge ggsn-pgw subscribers peer on page 1078 • show unified-edge ggsn-pgw subscribers on page 1095 • show unified-edge ggsn-pgw subscribers charging on page 1105
List of Sample Output	clear unified-edge ggsn-pgw subscribers charging gateway pgw on page 1077
Output Fields	No message is displayed on successful execution of this command; otherwise an error message is displayed.

Sample Output

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

clear unified-edge ggsn-pgw subscribers peer

Syntax	clear unified-edge ggsn-pgw subscribers peer gateway <i>gateway</i> remote-addr <i>remote-addr</i> <local-addr <i>local-addr</i>> <routing-instance <i>routing-instance</i>>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Clear the information for subscribers anchored on the specified GPRS tunneling protocol (GTP) peer on the specified gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW). The GTP peer can be a serving GPRS support node (SGSN) or a Serving Gateway (S-GW).
Options	<p>gateway <i>gateway</i>—Clear the subscribers for the specified GGSN or P-GW.</p> <p>remote-addr <i>remote-addr</i>—Clear the information for subscribers anchored on the peer with the specified IPv4 address.</p> <p>local-addr <i>local-addr</i>—(Optional) Clear the subscriber matching the specified local IPv4 address of the GGSN or P-GW on that interface.</p> <p>routing-instance <i>routing-instance</i>—(Optional) Clear the subscriber matching the specified routing instance.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• clear unified-edge ggsn-pgw subscribers on page 1075• clear unified-edge ggsn-pgw subscribers charging on page 1077• show unified-edge ggsn-pgw subscribers on page 1095
List of Sample Output	clear unified-edge ggsn-pgw subscribers peer gateway PGW remote-addr 11.11.11.2 on page 1078
Output Fields	No message is displayed on successful execution of this command; otherwise an error message is displayed.

Sample Output

clear unified-edge ggsn-pgw subscribers peer gateway PGW remote-addr 11.11.11.2	user@host> clear unified-edge ggsn-pgw subscribers peer gateway PGW remote-addr 11.11.11.2
--	--

show unified-edge ggsn-pgw apn service-mode

Syntax	show unified-edge ggsn-pgw apn service-mode <apn-name <i>apn-name</i> > <brief detail> <gateway <i>gateway</i> >
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Display the service mode information for an access point name (APN) for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If an APN is not specified, then the information for all APNs for one or more GGSNs or P-GWs is displayed.
Options	<p>none—(Same as brief) Display the APN service mode information in brief.</p> <p>apn-name <i>apn-name</i>—(Optional) Display the service mode information for the specified APN.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>gateway <i>gateway</i>—(Optional) Display the service mode information for the specified GGSN or P-GW.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show unified-edge ggsn-pgw service-mode on page 1086
List of Sample Output	show unified-edge ggsn-pgw apn service-mode brief on page 1080 show unified-edge ggsn-pgw apn service-mode detail on page 1080 show unified-edge ggsn-pgw apn service-mode apn-name apnv4-lp-vrf1-02 on page 1080
Output Fields	Table 71 on page 1079 lists the output fields for the show unified-edge ggsn-pgw apn service-mode command. Output fields are listed in the approximate order in which they appear.

Table 71: show unified-edge ggsn-pgw apn service-mode Output Fields

Field Name	Field Description
APN Name	Name of the APN.
Service Mode	Service mode for the APN: <ul style="list-style-type: none"> • Operational—APN is in operational mode. • Maintenance—APN is in maintenance mode.

Sample Output

```
show unified-edge user@host> show unified-edge ggsn-pgw apn service-mode brief
ggsn-pgw apn      Maintenance Mode
service-mode brief 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
apnr7.com	Operational
apnr8.com	Operational
apnr99.com	Operational
apnv4-gp-dvrf-01	Operational
[...output truncated...]	

```
show unified-edge user@host> show unified-edge ggsn-pgw apn service-mode detail
ggsn-pgw apn      APN Name      : apnr7.com
service-mode detail Service Mode  : Operational
```

```
APN Name      : apnr8.com
Service Mode  : Operational
```

```
APN Name      : apnr99.com
Service Mode  : Operational
```

```
APN Name      : apnv4-gp-dvrf-01
Service Mode  : Operational
```

```
[...output truncated...]
```

```
show unified-edge user@host> show unified-edge ggsn-pgw apn service-mode apn-name apnv4-lp-vrf1-02
ggsn-pgw apn      Maintenance Mode
service-mode       MM Active Phase - System is ready to accept configuration changes for all
apn-name           attributes of this object and its sub-hierarchies.
apnv4-lp-vrf1-02   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
apnv4-lp-vrf1-02	Operational

show unified-edge ggsn-pgw apn statistics

Syntax	show unified-edge ggsn-pgw apn statistics <i>apn-name</i> <i>apn-name</i> <i><gateway gateway></i>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Display the statistics for the specified access point name (APN) on one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then the statistics for the specified APN on all GGSNs and P-GWs are displayed.
Options	apn-name <i>apn-name</i> —Display the statistics for the specified APN. gateway <i>gateway</i> —(Optional) Display the statistics for the APN on the specified GGSN or P-GW.
Required Privilege Level	view
List of Sample Output	show unified-edge ggsn-pgw apn statistics apn-name apn-1 on page 1084
Output Fields	Table 72 on page 1081 lists the output fields for the show unified-edge ggsn-pgw apn statistics command. Output fields are listed in the approximate order in which they appear.

Table 72: show unified-edge ggsn-pgw apn statistics Output Fields

Field Name	Field Description
Gateway	Name of the GGSN or P-GW.
Control Plane APN Statistics	
Session establishment attempts	Number of attempted session establishments.
Successful session establishments	Number of successful session establishments.
MS/peer initiated session deactivations	Number of attempted deactivations initiated by the mobile station (MS) or the GTP peer.
Successful MS/peer initiated deactivations	Number of deactivations initiated by the MS or GTP peer that were successful.
Gateway initiated session deactivations	Number of attempted deactivations initiated by the broadband gateway.

Table 72: show unified-edge ggsn-pgw apn statistics Output Fields (continued)

Field Name	Field Description
Successful gateway initiated deactivations	Number of deactivations initiated by the broadband gateway that were successful.
MS initiated modification attempts	Number of attempted session or bearer modifications initiated by the MS or user equipment (UE).
Successful MS initiated modifications	Number of session or bearer modifications initiated by the MS or user equipment that were successful.
PGW/GGSN initiated modification attempts	Number of attempted session or bearer modifications initiated by the GGSN or P-GW.
Successful PGW/GGSN initiated modifications	Number of session or bearer modifications initiated by the GGSN or the P-GW that were successful.
User authentication statistics	<p>The following statistics related to user authentication are displayed:</p> <ul style="list-style-type: none"> • Authentication failures—Number of authentication failures. • Attempted authentications—Number of attempted authentications. • Successful authentications—Number of successful authentications.
Address allocation statistics	<p>The following statistics related to address allocation are displayed:</p> <ul style="list-style-type: none"> • dynamic IP allocation attempts—Number of attempted dynamic IP allocations. • dynamic IP allocation success—Number of successful dynamic IP allocations.
Charging statistics	<p>The following statistics related to charging are displayed:</p> <ul style="list-style-type: none"> • Number of CDRs allocated—Total number of Charging Data Records (CDRs) opened. • Number of partial CDRs allocated—Total number of partial CDRs opened. • Number of CDRs closed—Total number of CDRs closed. • Number of containers closed—Total number of containers closed.

Table 72: show unified-edge ggsn-pgw apn statistics Output Fields (continued)

Field Name	Field Description
Session Establishments Failed (by GTP cause)	Number of session establishments that failed, listed according to the following GTP cause codes (returned in the GTP Response message): <ul style="list-style-type: none"> • Others • Service unavailable • System failure • No resources • No address • Service denied • Authentication Fail • APN access denied
Data plane statistics	
Total packets violating MIF ACL	Total number of packets violating the mobile interface access control list (ACL) filters.
Total redirected mobile-to-mobile packets	Total number of mobile-to-mobile traffic packets redirected by the GGSN or P-GW.
Total redirected mobile-to-mobile bytes	Total number of octets of mobile-to-mobile traffic packets redirected by the GGSN or P-GW.
Miscellaneous Packet Statistics	
IPv6 Router Solicitations received	Number of IPv6 router solicitations received by the APN on the broadband gateway.
IPv6 Router Advertisement transmitted	Number of IPv6 router advertisements transmitted by the APN on the broadband gateway.
IPv6 Neighbor Solicitations received	Number of IPv6 neighbor solicitations received by the APN on the broadband gateway.
IPv6 Neighbor Advertisement transmitted	Number of IPv6 neighbor advertisements transmitted by the APN on the broadband gateway.
Data plane GTP statistics (Gn/S5/S8)	
Input packets	Number of incoming GTP data packets on the Gn, Gp, S5, and S8 interfaces.
Input bytes	Number of octets of incoming GTP data packets on the Gn, Gp, S5, and S8 interfaces.

Table 72: show unified-edge ggsn-pgw apn statistics Output Fields (*continued*)

Field Name	Field Description
Output packets	Number of outgoing GTP data packets on the Gn, Gp, S5, and S8 interfaces.
Output bytes	Number of octets of outgoing GTP data packets on the Gn, Gp, S5, and S8 interfaces.
Discarded packets	Number of discarded GTP data packets on the Gn, Gp, S5, and S8 interfaces.
Data plane GTP statistics (Gi)	
Input packets	Number of incoming GTP data packets on the Gi interface.
Input bytes	Number of octets of incoming GTP data packets on the Gi interface.
Output packets	Number of outgoing GTP data packets on the Gi interface.
Output bytes	Number of octets of outgoing GTP data packets on the Gi interface.
Discarded packets	Number of discarded GTP data packets on the Gi interface.

Sample Output

```

show unified-edge ggsn-pgw apn statistics apn-name apn-1
user@host> show unified-edge ggsn-pgw apn statistics apn-name apn-1
Gateway: PGW
Control plane APN statistics:
  Session establishment attempts: 1
  Successful session establishments: 1
  MS/peer initiated session deactivations: 0
  Successful MS/peer initiated deactivations: 0
  Gateway initiated session deactivations: 0
  Successful gateway initiated deactivations: 0
  MS initiated modification attempts: 0
  Successful MS initiated modifications: 0
  PGW/GGSN initiated modification attempts: 0
  Successful PGW/GGSN initiated modifications: 0
  User authentication statistics:
    Authentication failures: 0
    Attempted authentications: 0
    Successful authentications: 0
  Address allocation statistics:
    dynamic IP allocation attempts: 1
    dynamic IP allocation success: 1
  Charging statistics:
    Number of CDRs allocated: 0
    Number of partial CDRs allocated: 0
    Number of CDRs closed: 0
    Number of containers closed: 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 statistics:
    Total packets violating MIF ACL:      0
    Total redirected mobile-to-mobile packets: 0
    Total redirected 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:      5
    Input   bytes:        2560
    Output  packets:      5
    Output  bytes:        2560
    Discarded packets:    0
Data plane GTP statistics (Gi):
    Input   packets:      5
    Input   bytes:        2560
    Output  packets:      5
    Output  bytes:        2560
    Discarded packets:    0
```

show unified-edge ggsn-pgw service-mode

Syntax	show unified-edge ggsn-pgw service-mode <brief detail> <gateway gateway-name>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Display the service mode information for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then the service mode information for all the GGSNs and P-GWs is displayed.
Options	<p>none—(Same as brief) Display the service mode information in brief.</p> <p>brief detail —(Optional) Display the specified level of output.</p> <p>gateway gateway-name—(Optional) Display service mode information for the specified GGSN or P-GW.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show unified-edge ggsn-pgw apn service-mode on page 1079
List of Sample Output	show unified-edge ggsn-pgw service-mode brief on page 1086 show unified-edge ggsn-pgw service-mode detail on page 1087
Output Fields	Table 73 on page 1086 lists the output fields for the show unified-edge ggsn-pgw service-mode command. Output fields are listed in the approximate order in which they appear.

Table 73: show unified-edge ggsn-pgw service-mode Output Fields

Field Name	Field Description
Gateway Name	Name of the GGSN or P-GW.
Service Mode	Service mode for the gateway: <ul style="list-style-type: none"> • Operational—Gateway is in operational mode. • Maintenance—Gateway is in maintenance mode.

Sample Output

```

show unified-edge ggsn-pgw service-mode brief
user@host> show unified-edge ggsn-pgw service-mode brief
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
PGW	Operational
PGW2	Operational

```
show unified-edge ggsn-pgw service-mode detail
user@host> show unified-edge ggsn-pgw service-mode detail
Service Mode Status
Gateway Name      : PGW
Service Mode      : Operational
Service Mode Status
Gateway Name      : PGW2
Service Mode      : Operational
```

show unified-edge ggsn-pgw statistics

Syntax	show unified-edge ggsn-pgw statistics <gateway gateway>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Display the statistics for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then statistics for all GGSNs and P-GWs are displayed.
Options	gateway gateway —(Optional) Display the statistics for the specified GGSN or P-GW.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear unified-edge ggsn-pgw statistics on page 1074
List of Sample Output	show unified-edge ggsn-pgw statistics on page 1089
Output Fields	Table 74 on page 1088 lists the output fields for the show unified-edge ggsn-pgw statistics command. Output fields are listed in the approximate order in which they appear.

Table 74: show unified-edge ggsn-pgw statistics Output Fields

Field Name	Field Description
Gateway	Name of the GGSN or P-GW.
Control Plane Statistics	
Session establishment attempts	Number of attempted session establishments.
Successful session establishments	Number of successful session establishments.
MS/peer initiated session deactivations	Number of attempted deactivations initiated by the mobile station (MS) or GPRS tunneling protocol (GTP) peer.
Successful MS/peer initiated deactivations	Number of deactivations initiated by the MS or GTP peer that were successful.
Gateway initiated session deactivations	Number of attempted deactivations initiated by the broadband gateway.

Table 74: show unified-edge ggsn-pgw statistics Output Fields (*continued*)

Field Name	Field Description
Successful gateway initiated deactivations	Number of deactivations initiated by the broadband gateway that were successful.
Data Plane Global statistics	
Source address violation packets	Number of packets with an incorrect source address.
Source address violation bytes	Number of octets with an incorrect source address.
Total packets rcvd with non-existent TEIDs	Total number of packets received with nonexistent tunnel endpoint identifiers (TEIDs).
Data Plane GTP Statistics (Gn/S5/S8)	
Input packets	Number of incoming GTP data packets on the Gn, Gp, S5, and S8 interfaces.
Input bytes	Number of octets of incoming GTP data packets on the Gn, Gp, S5, and S8 interfaces.
Output packets	Number of outgoing GTP data packets on the Gn, Gp, S5, and S8 interfaces.
Output bytes	Number of octets of outgoing GTP data packets on the Gn, Gp, S5, and S8 interfaces.
Discarded packets	Number of discarded GTP data packets on the Gn, Gp, S5, and S8 interfaces.
Data Plane GTP statistics (Gi)	
Input packets	Number of incoming GTP data packets on the Gi interface.
Input bytes	Number of octets of incoming GTP data packets on the Gi interface.
Output packets	Number of outgoing GTP data packets on the Gi interface.
Output bytes	Number of octets of outgoing GTP data packets on the Gi interface.
Discarded packets	Number of discarded GTP data packets on the Gi interface

Sample Output

```

show unified-edge ggsn-pgw statistics user@host> show unified-edge ggsn-pgw statistics
Control plane statistics:
  Session establishment attempts:      187501
  Successful session establishments:    187501
  MS/peer initiated session deactivations: 46878
  Successful MS/peer initiated deactivations: 46878
  Gateway initiated session deactivations: 0

```

```
Successful gateway initiated deactivations: 0
Data plane global statistics:
  Source address violation packets:          0
  Source address violation bytes:           0
  Total packets rcvd with non-existent TEIDs: 0
Data plane GTP statistics (Gn/S5/S8):
  Input   packets:      2999505
  Input   bytes:        2111435520
  Output  packets:      221199
  Output  bytes:        14156736
  Discarded packets:    0
Data plane GTP statistics (Gi):
  Input   packets:      221199
  Input   bytes:        14156736
  Output  packets:      2999505
  Output  bytes:        2111435520
  Discarded packets:    0
```


show unified-edge ggsn-pgw status

Syntax `show unified-edge ggsn-pgw status`
`<apn-name apn-name>`
`<brief | detail>`
`<fpc-slot fpc-slot>`
`<gateway gateway>`
`<gtpv1-arp gtpv1-arp>`
`<gtpv2-priority-level gtpv2-priority-level>`
`<pic-slot pic-slot>`
`<qci qci>`
`<rat-type (eutran | gan | geran | hspa | others | utran | wlan)>`
`<session-state>`
`<traffic-class (background | conversational | interactive | streaming)>`
`<traffic-handling-priority traffic-handling-priority>`

Release Information Command introduced in Junos OS Mobility Release 11.2W.

Description Display the status information, such as the number of subscribers, active sessions, and so on, for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then statistics for all GGSNs and P-GWs is displayed.

Options `none`—(Same as `brief`) Display the status information in brief.

`apn-name apn-name`—(Optional) Display the status information for the specified access point name (APN).

`brief | detail`—(Optional) Display the specified level of output.

`fpc-slot fpc-slot`—(Optional) Display the status information for the specified FPC slot number.

`gateway gateway`—(Optional) Display the status information for the specified GGSN or P-GW.

`gtpv1-arp gtpv1-arp`—(Optional) Display the status information for the GTPv1 Allocation and Retention Priority (ARP) value specified. You can specify a GTPv1 ARP value of 1 through 3.

`gtpv2-priority-level gtpv2-priority-level`—(Optional) Display the status information for the GTPv2 priority specified. You can specify a priority of 1 through 15.

`pic-slot pic-slot`—(Optional) Display the status information for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

`qci qci`—(Optional) Display the status information for the specified QoS Class Identifier (QCI). You can specify a QCI of 1 through 9.

`rat-type (eutran | gan | geran | hspa | others | utran | wlan)`—(Optional) Display the status information for the specified Radio Access Technology (RAT).

session-state—(Optional) Display the session state of subscriber sessions anchored on one or more GGSNs or P-GWs

traffic-class (background | conversational | interactive | streaming)—(Optional) Display the status information for the specified conversational class.

traffic-handling-priority *traffic-handling-priority*—(Optional) Display the status information for the specified traffic handling priority. You can specify a priority from 1 through 3.

Required Privilege Level view

Related Documentation • [show unified-edge ggsn-pgw status preemption-list on page 1177](#)

List of Sample Output [show unified-edge ggsn-pgw status on page 1093](#)
[show unified-edge ggsn-pgw status detail on page 1093](#)
[show unified-edge ggsn-pgw status session-state detail on page 1094](#)

Output Fields [Table 75 on page 1092](#) lists the output fields for the **show unified-edge ggsn-pgw status** command. Output fields are listed in the approximate order in which they appear.

Table 75: show unified-edge ggsn-pgw status Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the GGSN or P-GW.	All levels none
FPC SLOT	FPC slot number of the interface for which the status information is displayed.	detail
PIC SLOT	PIC slot number of the FPC for which the status information is displayed.	detail
State	State of the services PIC on the GGSN or P-GW: <ul style="list-style-type: none"> • Standalone • Active—Services PIC is an active member. • Backup—Services PIC is a backup. 	detail
Active Subscribers	Number of active subscribers.	All levels none
Active Sessions	Number of active sessions.	All levels none
Active Bearers	Number of active bearers or Packet Data Protocol (PDP) contexts.	All levels none
CPU Load (%)	Percentage of the CPU load.	All levels none

Table 75: show unified-edge ggsn-pgw status Output Fields (*continued*)

Field Name	Field Description	Level of Output
Memory Load (%)	Percentage of the memory load.	All levels none
State The following information about the session state is displayed:		
Established	Number of sessions established.	session-state
Deleting	Number of sessions being deleted.	session-state
Updating bearer	Number of sessions for which the bearers or PDP contexts are being updated.	session-state
Authorizing	Number of sessions waiting for initial authorization.	session-state
Acquiring address	Number of sessions for which the IP address is being acquired.	session-state

Sample Output

```

show unified-edge user@host> show unified-edge ggsn-pgw status
ggsn-pgw status   Gateway: PGW
                  Mobile gateway status:
                  Active Subscribers   :           1
                  Active Sessions      :           1
                  Active Bearers       :           1
                  CPU Load (%)         :           0
                  Memory Load (%)      :          39

show unified-edge user@host> show unified-edge ggsn-pgw status detail
ggsn-pgw status detail Gateway: PGW
                  Mobile gateway status:

                  FPC SLOT: 2 PIC SLOT: 0
                  State           :           Active
                  Active Subscribers :           0
                  Active Sessions  :           0
                  Active Bearers   :           0
                  CPU Load (%)     :           0
                  Memory Load (%)  :          39
                  Mobile gateway status:

                  FPC SLOT: 2 PIC SLOT: 1
                  State           :           Backup
                  Active Subscribers :           0
                  Active Sessions  :           0
                  Active Bearers   :           0
                  CPU Load (%)     :           0
                  Memory Load (%)  :          40

```

```
show unified-edge ggsn-pgw status session-state detail
user@host> show unified-edge ggsn-pgw status session-state detail
Gateway: PGW
Mobile gateway status of fpc slot: 11 pic slot: 0
Established      :          668829
Deleting        :           0
Updating bearer  :           0
Authorizing      :           0
Acquiring address :           0

Mobile gateway status of fpc slot: 11 pic slot: 1
Established      :          669207
Deleting        :           0
Updating bearer  :           0
Authorizing      :           0
Acquiring address :           0

[...output truncated...]
```

show unified-edge ggsn-pgw subscribers

Syntax `show unified-edge ggsn-pgw subscribers`
 `<anchored-services>`
 `<apn apn-name>`
 `<brief | detail | extensive>`
 `<fpc-slot fpc-slot>`
 `<gateway gateway>`
 `<gtp-ver gtp-ver>`
 `<gtpv1-arp gtpv1-arp>`
 `<gtpv2-priority-level gtpv2-priority-level>`
 `<imsi imsi>`
 `<msisdn msisdn>`
 `<peer peer>`
 `<pic-slot pic-slot>`
 `<qci qci>`
 `<routing-instance routing-instance>`
 `<service-fpc-slot fpc-slot>`
 `<service-pic-slot pic-slot>`
 `<session-state (acquire-address | authorizing | bearer-update | deleting | established)>`
 `<traffic-class (background | conversational | interactive | streaming)>`
 `<traffic-handling-priority traffic-handling-priority>`
 `<v4-addr v4-addr>`
 `<v6-addr v6-addr>`

Release Information Command introduced in Junos OS Mobility Release 11.2W.
 Support for the **anchored-services**, **service-fpc-slot**, and **service-pic-slot** attributes introduced in Junos OS Mobility Release 11.4W.

Description Display the subscriber information one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then subscriber information for all GGSNs and P-GWs is displayed.

Options **none**—(Same as **brief**) Display the subscriber information in brief.

anchored-services—(Optional) Display the information for subscribers who are using subscriber-aware services and who are anchored on a services PIC.

apn *apn-name*—(Optional) Display the subscriber information for the specified access point name (APN).

brief | detail | extensive —(Optional) Display the specified level of output.

fpc-slot *fpc-slot*—(Optional) Display the subscriber information for the specified FPC slot number.

gateway *gateway*—(Optional) Display the subscriber information for the specified gateway name.

gtp-ver *gtp-ver*—(Optional) Display the subscriber information for the GTP version number (0 through 2) specified.

gtpv1-arp *gtpv1-arp*—(Optional) Display the subscriber information for the GTPv1 Allocation and Retention Priority (ARP) value specified. You can specify a GTPv1 ARP value of 1 through 3.

gtpv2-priority-level *gtpv2-priority-level*—(Optional) Display the subscriber information for the GTPv2 priority specified. You can specify a priority of 1 through 15.

imsi *imsi*—(Optional) Display the subscriber information for the specified International Mobile Subscriber Identity (IMSI).

msisdn *msisdn*—(Optional) Display the subscriber information for the specified Mobile Station ISDN (MSISDN) number.

peer *peer*—(Optional) Display the subscriber information for the specified peer IP address.

pic-slot *pic-slot*—(Optional) Display the subscriber information for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

qci *qci*—(Optional) Display the subscriber information for the specified QoS Class Identifier (QCI).

routing-instance *routing-instance*—(Optional) Display the subscriber information for the specified routing instance.

service-fpc-slot *fpc-slot* **service-pic-slot** *pic-slot*—(Optional) Display the information for subscribers who are using subscriber-aware services and who are anchored on the services PIC in the specified FPC and PIC slots.



.....
NOTE: You must specify the **anchored-services** option along with the **service-fpc-slot** and **service-pic-slot** options.
.....

session-state (**acquire-address** | **authorizing** | **bearer-update** | **deleting** | **established**)—(Optional) Display the subscriber information for the specified session state. You can specify the following session states:

- **acquire-address**—Sessions for which the IP address is being acquired.
- **authorizing**—Sessions waiting for initial authorization.
- **bearer-update**—Sessions which are being updated.
- **deleting**—Sessions being deleted.
- **established**—Sessions already established.

traffic-class (**background** | **conversational** | **interactive** | **streaming**)—(Optional) Display the subscriber information for the specified conversational class.

traffic-handling-priority *traffic-handling-priority*—(Optional) Display the subscriber information for the specified traffic handling priority. You can specify a priority from 1 through 3.

v4-addr v4-addr—(Optional) Display the subscriber information for the specified IPv4 address of the subscriber's user equipment (UE).

v6-addr v6-addr—(Optional) Display the subscriber information for the specified IPv6 address of the subscriber's user equipment.

Required Privilege Level view

Related Documentation

- [clear unified-edge ggsn-pgw subscribers on page 1075](#)
- [clear unified-edge ggsn-pgw subscribers charging on page 1077](#)
- [clear unified-edge ggsn-pgw subscribers peer on page 1078](#)

List of Sample Output

- [show unified-edge ggsn-pgw subscribers on page 1103](#)
- [show unified-edge ggsn-pgw subscribers detail on page 1103](#)
- [show unified-edge ggsn-pgw subscribers extensive on page 1103](#)

Output Fields [Table 76 on page 1097](#) lists the output fields for the **show unified-edge ggsn-pgw subscribers** command. Output fields are listed in the approximate order in which they appear.

Table 76: show unified-edge ggsn-pgw subscribers Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the GGSN or P-GW.	All levels none
IMSI	IMSI of the subscriber's user equipment.	brief none
MSISDN	MSISDN number of the subscriber's user equipment.	brief none
Subscriber Address	IP address of the subscriber's user equipment.	brief none
Peer Address	IP address of the GTP peer through which the subscriber is connected to the broadband gateway.	brief none
APN	Access point name (APN), on the broadband gateway, to which the subscriber is attached.	brief none
Subscriber Information:		
IMSI	IMSI of the subscriber's user equipment.	detail extensive

Table 76: show unified-edge ggsn-pgw subscribers Output Fields (*continued*)

Field Name	Field Description	Level of Output
IMEI	International Mobile Station Equipment Identity (IMEI) of the subscriber's user equipment.	detail
		extensive
MSISDN	MSISDN number of the subscriber's user equipment.	extensive
Time Zone	Time zone to which the subscriber belongs.	extensive
(DST)	Daylight saving time applicable within the time zone.	extensive
RAT Type	Type of Radio Access Technology (RAT) used.	detail
		extensive
Status	Status of the subscriber; that is, whether the subscriber is a visitor, home subscriber, or a roamer.	detail
		extensive
MCC	Mobile country code (MCC) of the subscriber.	extensive
MNC	Mobile network code (MNC) of the subscriber.	extensive
LAC	Location area code (LAC) of the subscriber.	extensive
CI	Cell Identity (CI) of the subscriber.	extensive
SAC	Service area code (SAC) of the subscriber.	extensive
RAC	Routing area code (RAC) of the subscriber.	extensive
TAC	Tracking area code (TAC) of the subscriber.	extensive
ECI	E-UTRAN Cell identifier (ECI) of the subscriber.	extensive
PDN Session:		
APN name	Access point name for the Packet Data Network (PDN) session.	detail
		extensive
IPv4 Address	IPv4 address of the subscriber.	detail
		extensive
IPv6 Address	IPv6 address of the subscriber.	detail
		extensive

Table 76: show unified-edge ggsn-pgw subscribers Output Fields (*continued*)

Field Name	Field Description	Level of Output
GTP Version	GTP version used for the control plane.	detail
		extensive
Session Duration	Duration of the PDP session.	detail
		extensive
Local Control address	Local IPV4 address of the broadband gateway to which the peer (SGSN or S-GW) will send the control messages for the subscriber.	detail
		extensive
Remote Control address	IP address of the peer (SGSN or S-GW) to which the broadband gateway will send control messages for the subscriber.	detail
		extensive
TEID Control Local	Tunnel endpoint identifier (TEID) allocated locally by the broadband gateway for the control plane or signaling messages. The control peers (SGSN or S-GW) send this TEID in all control messages to the broadband gateway.	detail
		extensive
TEID Control Remote	Control TEID for the session, which is allocated by the remote control peer (SGSN or S-GW). The broadband gateway sends this TEID in the GTP header in all control messages to the peer.	detail
		extensive
Peer CSID	Connection Set Identifier (CSID) allocated by the GTP peer (S-GW).	extensive
Remote CSID	CSID allocated by the Mobility Management Entity (MME). It identifies the connection set on the MME to which the session belongs.	extensive
Addressing scheme	Addressing scheme used for IP address allocation.	extensive
Selection mode	Selection mode configured for the APN on the broadband gateway.	extensive
Session PIC	FPC and PIC slots for the session PIC on which the subscriber control session is anchored.	detail
		extensive
Anchor PFE	FPC and PIC slots for the anchor Packet Forwarding Engine for the PDP session.	detail
		extensive
Service PIC	FPC and PIC slot numbers of the services PIC on which the subscriber services are anchored.	detail
		extensive
Service PFE (ifd/vpfe-id)	Packet Forwarding Engine on which services are applied. The physical interface and the virtual Packet Forwarding Engine identifier are also displayed.	detail
		extensive

Table 76: show unified-edge ggsn-pgw subscribers Output Fields (*continued*)

Field Name	Field Description	Level of Output
Session State	State of the subscriber session on the signaling plane.	detail
		extensive
Direct Tunnel	Status of the GTPv1 direct tunnel: enabled or disabled.	extensive
Serving network	The following information about the PDN serving the subscriber is displayed: <ul style="list-style-type: none">• MCC—Mobile country code of the network.• MNC—Mobile network code of the network.	extensive
Negotiated APN AMBR	The aggregate maximum bit rate (AMBR) negotiated for the PDP session is displayed for the following: <ul style="list-style-type: none">• Downlink—Negotiated AMBR in the downlink direction.• Uplink—Negotiated AMBR in the uplink direction.	detail
		extensive
Requested APN AMBR	The AMBR requested by the user equipment for the session is displayed for the following: <ul style="list-style-type: none">• Downlink—Requested AMBR in the downlink direction.• Uplink—Requested AMBR in the uplink direction.	extensive
Bearer:		
NSAPI/EBI	Network Service Access Point Identifier (NSAPI) or the Evolved Packed System Bearer ID (EBI) for the session.	detail
		extensive
Charging ID	Charging ID for the session. The charging ID is the unique bearer identity sent in accounting messages and in Charging Data Records (CDRs).	detail
		extensive
Local Data address	IP address of the broadband gateway to which the peer sends the data packets for the PDP context or bearer.	detail
		extensive
Remote Data address	IP address of the peer to which the broadband gateway sends the data packets for the PDP context or bearer.	detail
		extensive
Local TEID	Data TEID allocated by the broadband gateway which identifies the data tunneling endpoint for all data packets coming in from the data peer. This is sent in the GTP header for all data packets coming from the peer GTP nodes (SGSN or S-GW).	detail
		extensive
Remote TEID	Data TEID allocated by the data plane peer for the session which identifies the data tunneling endpoint for all data packets sent from the broadband gateway to the remote peer.	detail
		extensive
Bearer State	Represents the state of the subscriber in the forwarding or data plane. This parameter is used internally by the broadband gateway.	detail
		extensive

Table 76: show unified-edge ggsn-pgw subscribers Output Fields (*continued*)

Field Name	Field Description	Level of Output
Substate	Represents the substate of the subscriber in the forwarding or data plane. This parameter is used internally by the broadband gateway.	detail extensive
Idle Timeout	<p>Idle timeout for the session, in minutes. The following information regarding the idle timeout is displayed in parentheses:</p> <ul style="list-style-type: none"> Internal profile ID for idle timeout on the Packet Forwarding Engine. Current timeout count that the Packet Forwarding Engine reported for the subscriber. Total timeout count that the Packet Forwarding Engine needs to report to be considered as an idle timeout for the subscriber. 	detail extensive
AAA Interim Interval	<p>Authentication, authorization, and accounting (AAA) interim account timer, in minutes. The following information regarding AAA interim interval is displayed in parentheses:</p> <ul style="list-style-type: none"> Internal profile ID for the AAA interim account timer on the Packet Forwarding Engine. Current timeout count that Packet Forwarding Engine reported for the subscriber. Total timeout count that the Packet Forwarding Engine needs to report to be considered as AAA interim accounting interval reached for the subscriber. 	detail extensive
Negotiated QoS Parameters	<p>The following parameters (negotiated by the user equipment) related to quality of service (QoS) are displayed:</p> <ul style="list-style-type: none"> QCI—QoS Class Identifier. ARP: (PL/PVI/PCI) The following parameters related to ARP are displayed: <ul style="list-style-type: none"> Priority level (PL) Preemption Vulnerability Indicator (PVI) Preemption Capability Indicator (PCI) Forwarding Class—The forwarding class. Loss Priority—Packet loss priority 	detail extensive
Requested QoS Parameters	<p>The following parameters (requested by the user equipment) related to QoS are displayed:</p> <ul style="list-style-type: none"> QCI—QoS Class Identifier ARP: (PL/PVI/PCI) The following parameters related to ARP are displayed: <ul style="list-style-type: none"> Priority Level (PL) Preemption Vulnerability Indicator (PVI) Preemption Capability Indicator (PCI) 	detail extensive

Table 76: show unified-edge ggsn-pgw subscribers Output Fields (*continued*)

Field Name	Field Description	Level of Output
Charging information	The following information related to charging is displayed:	detail
	<ul style="list-style-type: none"> • Profile ID—ID of the charging profile associated with the bearer. • Profile name—Name of the charging profile associated with the bearer. • State—Current charging state for the bearer. • Previous State—Previous charging state for the bearer. • Profile selection criteria—Selection source (home, visitor, roamer, and default) for the charging profile for the bearer. This field is displayed only when the command is executed with the extensive option. • Details—Current charging flag information for the bearer, which indicates what charging features are enabled. For example, Accounting enabled, offline bearer indicates that accounting and offline charging are enabled for the bearer. 	extensive
Offline charging information	<p>The following offline charging information is displayed:</p> <ul style="list-style-type: none"> • Current service data container sequence number—Sequence number of the current local service data container. • Current partial record sequence number—Sequence number of the current partial record CDR. • Number of CDRs closed—Number of closed CDRs generated. • Number of containers closed—Number of containers closed. 	extensive
Rating group information	The following information related to the rating group is displayed:	detail
	<ul style="list-style-type: none"> • Rating group—Default rating group associated with the bearer. • Service ID—Service identifier of the rating group. • Trigger profile—Trigger profile number associated with the rating group. This field is displayed only when the command is executed with the extensive option. • Change condition bitmask—Rating group trigger change condition bitmask. This field is displayed only when the command is executed with the extensive option. • Action-id-bitmask—Charging action ID bitmask. This field is displayed only when the command is executed with the extensive option. • Signal bitmask—Rating group trigger signal condition bitmask. This field is displayed only when the command is executed with the extensive option. • Last signal bitmask—Previous rating group trigger signal condition bitmask. This field is displayed only when the command is executed with the extensive option. • Details—Trigger flag information. • Last statistics collection time—Time when the last control plane recorded statistics for the subscriber. This field is displayed only when the command is executed with the extensive option. The following information from the statistics received from the Packet Forwarding Engine is displayed: <ul style="list-style-type: none"> • Uplink packets—Number of packets handled in the uplink direction. • Downlink packets—Number of packets handled in the downlink direction. • Uplink bytes—Number of bytes handled in the uplink direction. • Downlink bytes—Number of bytes handled in the downlink direction. 	extensive

Sample Output

```

show unified-edge user@host> show unified-edge ggsn-pgw subscribers
ggsn-pgw subscribers Gateway: PGW

```

IMSI	MSISDN	Subscriber Address	Peer Address	APN
123213213123256	1926737745	20.20.4.1	200.6.88.2	jnpr-sunnyvale

```

show unified-edge user@host> show unified-edge ggsn-pgw subscribers detail
ggsn-pgw subscribers Gateway: PGW
detail

```

Subscriber Information:

IMSI: 123213213123256 IMEI: 1122334455667788

RAT Type: E-UTRAN Status: Visitor

PDN Session:

APN name: jnpr-sunnyvale

IPv4 Address: 20.20.4.1 IPv6 Address: None

GTP Version: 2 Session Duration: 1:07

Local Control address: 200.6.88.1 Remote Control address: 200.6.88.2

TEID Control Local: 0x19000000 TEID Control Remote: 0x9000c00

Session PIC: 5 /1 (FPC/PIC) Anchor PFE: 1 /0 (FPC/PIC)

Service PIC: 0 /0 (FPC/PIC) Service PFE: 0 /0 (ifd/vpfe-id)

Session State: Established

Negotiated APN AMBR: Downlink: 128 kbps Uplink: 128 kbps

Bearer:

Bearer:

NSAPI/EBI: 5 Charging ID: 0x19000000

Local Data address: 200.6.88.1 Remote Data address: 200.6.88.2

Local TEID: 0x28110000 Remote TEID: 0x310000

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: 1 /0 /0 (PL/PVI/PCI)

Forwarding Class: None Loss Priority: None

Requested QoS Parameters:

QCI: 5 ARP: 1 /0 /0 (PL/PVI/PCI)

Charging information: Profile ID: 1 Profile name: p_juniper

State: Ready Previous State: Ga

Details: Offline bearer

Rating group information:

Rating group: 0 Service id: 0

Details: Bearer trigger, Offline RG

```

show unified-edge user@host> show unified-edge ggsn-pgw subscribers extensive
ggsn-pgw subscribers Gateway: PGW
extensive

```

Subscriber Information:

IMSI: 123213213123256 IMEI: 1122334455667788

MSISDN: 1926737745 Time Zone: GMT (DST): None

RAT Type: E-UTRAN Status: Visitor

MCC: 450 MNC: 51

LAC: 0x37 CI: 0xffff SAC: 0x0 RAC: 0x0 TAC: 0x0 ECI: 0x0

PDN Session:

APN name: jnpr-sunnyvale

IPv4 Address: 20.20.4.1 IPv6 Address: None

GTP Version: 2 Session Duration: 1:32

Local Control address: 200.6.88.1 Remote Control address: 200.6.88.2

TEID Control Local: 0x19000000 TEID Control Remote: 0x9000c00

```

Peer CSID: 49                                     Remote CSID: 6
Addressing scheme: Local                           Selection mode: sub verified
Session PIC: 5 /1 (FPC/PIC)                       Anchor PFE: 1 /0 (FPC/PIC)
Service PIC: 0 /0 (FPC/PIC)                       Service PFE: 0 /0 (ifd/vpfe-id)
Session State: Established
Direct Tunnel: Disabled                           Serving network: MCC: 123 MNC :567
Negotiated APN AMBR: Downlink: 128 kbps           Uplink: 128 kbps
Requested APN AMBR: Downlink: 128 kbps            Uplink: 128 kbps

Bearer:
Bearer:
NSAPI/EBI: 5                                     Charging ID: 0x19000000
Local Data address: 200.6.88.1                   Remote Data address: 200.6.88.2
Local TEID: 0x28110000                           Remote TEID: 0x310000
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: 1 /0 /0 (PL/PVI/PCI)
    Forwarding Class: None                         Loss Priority: None
Requested QoS Parameters:
    QCI: 5                                         ARP: 1 /0 /0 (PL/PVI/PCI)
Charging information: Profile ID: 1                Profile name: p_juniper
    State: Ready                                   Previous State: Ga
    Profile selection criteria: Static default
    Details: Offline bearer
Offline charging information:
    Current service data container sequence number: 0
    Current partial record sequence number          : 0
    Number of CDRs closed                           : 0
    Number of containers closed                      : 0
Rating group information:
    Rating group: 0 Service id: 0
    Action ID: 0x3000000                           Trigger profile: 1
    Change condition bitmask: 0x0                   Action-id-bitmask: 0x0
    Signal bitmask: 0x0                             Last signal bitmask: 0x0
    Details: Bearer trigger, Offline RG
    Collection time: None collected

```

show unified-edge ggsn-pgw subscribers charging

Syntax `show unified-edge ggsn-pgw subscribers charging gateway gateway`
`<brief | detail | extensive>`
`<charging-profile charging-profile>`
`<fpc-slot fpc-slot>`
`<pic-slot pic-slot>`
`<transport-profile transport-profile>`

Release Information Command introduced in Junos OS Mobility Release 11.2W.

Description Display the subscribers matching the specified charging profile or transport profile on the specified gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW).

Options `gateway gateway`—Display the subscriber information for the specified gateway name.

`brief | detail | extensive` —(Optional) Display the specified level of output.

`charging-profile charging-profile`—(Optional) Display the subscribers matching the specified charging profile name.



NOTE: You must specify either a charging profile or a transport profile to execute this command.

`fpc-slot fpc-slot`—(Optional) Display the subscriber information for the specified FPC slot number.

`pic-slot pic-slot`—(Optional) Display the subscriber information for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

`transport-profile transport-profile`—(Optional) Display the subscribers matching the specified transport profile name.



NOTE: You must specify either a charging profile or a transport profile to execute this command.

Required Privilege Level view

Related Documentation

- [clear unified-edge ggsn-pgw subscribers charging on page 1077](#)
- [show unified-edge ggsn-pgw subscribers on page 1095](#)

List of Sample Output [show unified-edge ggsn-pgw subscribers charging gateway gw1 charging-profile cp1 brief on page 1106](#)
[show unified-edge ggsn-pgw subscribers charging gateway gw1 charging-profile cp1 detail on page 1106](#)
[show unified-edge ggsn-pgw subscribers charging gateway gw1 charging-profile cp1 extensive on page 1107](#)

Output Fields Refer to the output fields for the [show unified-edge ggsn-pgw subscribers](#) command, which is the same as the output fields for the [show unified-edge ggsn-pgw subscribers charging](#) command.

Sample Output

```
show unified-edge ggsn-pgw subscribers charging gateway gw1 charging-profile cp1 brief
user@host> show unified-edge ggsn-pgw subscribers charging gateway gw1 charging-profile cp1 brief
      IMSI                MSISDN                Subscriber Address      Peer Address      APN
111222330000003      444550000003      200.1.40.1          50.50.50.3      internet123
```

```
show unified-edge ggsn-pgw subscribers charging gateway gw1 charging-profile cp1 detail
user@host> show unified-edge ggsn-pgw subscribers charging gateway gw1 charging-profile cp1 detail
Subscriber Information:
  IMSI: 111222330000003      IMEI: None
  RAT Type: Unknown          Status: Visitor
PDN Session:
  APN name: internet123
  IPv4 Address: 200.1.40.1      IPv6 Address: None
  GTP Version: 1                Session Duration: 6:01:12
  Local Control address: 200.1.88.1 Remote Control address: 50.50.50.3
  TEID Control Local: 0x10000801 TEID Control Remote: 0x3
  Session PIC: 5 /0 (FPC/PIC)   Anchor PFE: 0 /0 (FPC/PIC)
  Service PIC: 0 /0 (FPC/PIC)   Service PFE: 0 /0 (ifd/vpfe-id)
  Session State: Established
Bearer:
Bearer:
  NSAPI/EBI: 5                Charging ID: 0x10000401
  Local Data address: 200.1.88.1 Remote Data address: 50.50.50.3
  Local TEID: 0x14100800       Remote TEID: 0x2713
  Bearer State: Established     Substate: -
  Idle Timeout: 0 min(0 -0,0)   AAA Interim Interval: 0 min(0 -0,0)
Negotiated QoS Parameters:
  Traffic Class: Interactive    ARP: 1
  Traffic Handling Priority: 1   Transfer Delay: 0
  MBR Uplink: 2048 kbps         MBR Downlink: 2048 kbps
                                Signaling Indicator: 0
                                Loss Priority: None
Requested QoS Parameters:
  Traffic Class: Interactive    ARP: 1
  Traffic Handling Priority: 1   Transfer Delay: 0
  MBR Uplink : 2048 kbps        MBR Downlink: 2048 kbps
                                Signaling Indicator: 0
Charging information: Profile ID: 1 Profile name: cp1
  State: Ready                  Previous State: Ga
  Details: Offline bearer
Rating group information:
  Rating group: 0 Service id: 0
```


Details: Bearer trigger, Offline RG

show unified-edge
ggsn-pgw subscribers
charging gateway gw1
charging-profile cp1
extensive

user@host> show unified-edge ggsn-pgw subscribers charging gateway gw1 charging-profile cp1 extensive

```
Subscriber Information:
  IMSI: 111222330000003      IMEI: None
  MSISDN: 444550000003      Time Zone: GMT      (DST): None
  RAT Type: Unknown          Status: Visitor
  MCC: None MNC: None
  LAC: 0x0 CI: 0x0          SAC: 0x0 RAC: 0x0 TAC: 0x0 ECI: 0x0
PDN Session:
  APN name: internet123
  IPv4 Address: 200.1.40.1    IPv6 Address: None
  GTP Version: 1              Session Duration: 6:01:19
  Local Control address: 200.1.88.1 Remote Control address: 50.50.50.3
  TEID Control Local: 0x10000801 TEID Control Remote: 0x3
  Addressing scheme: Local    Selection mode: MS or network provided APN,
subscription verified
  Session PIC: 5 /0 (FPC/PIC) Anchor PFE: 0 /0 (FPC/PIC)
  Service PIC: 0 /0 (FPC/PIC) Service PFE: 0 /0 (ifd/vpfe-id)
  Session State: Established
  Direct Tunnel: Disabled     Serving network: MCC: 123 MNC :456
Bearer:
Bearer:
  NSAPI/EBI: 5                Charging ID: 0x10000401
  Local Data address: 200.1.88.1 Remote Data address: 50.50.50.3
  Local TEID: 0x14100800      Remote TEID: 0x2713
  Bearer State: Established    Substate: -
  Idle Timeout: 0 min(0 -0,0) AAA Interim Interval: 0 min(0 -0,0)
Negotiated QoS Parameters:
  Traffic Class:Interactive    ARP: 1
  Traffic Handling Priority:1   Transfer Delay: 0
  MBR Uplink: 2048             kbps MBR Downlink: 2048 kbps
                                   Signaling Indicator: 0
                                   Loss Priority: None
Forwarding Class: None
Requested QoS Parameters:
  Traffic Class: Interactive    ARP: 1
  Traffic Handling Priority: 1   Transfer Delay: 0
  MBR Uplink : 2048             kbps MBR Downlink: 2048 kbps
                                   Signaling Indicator: 0
Charging information: Profile ID: 1 Profile name: cp1
  State: Ready                  Previous State: Ga
  Profile selection criteria: Static default
  Details: Offline bearer
Offline charging information:
  Current service data container sequence number: 0
  Current partial record sequence number : 0
  Number of CDRs closed : 0
  Number of containers closed : 0
Rating group information:
  Rating group: 0 Service id: 0
  Action ID: 0x2000401          Trigger profile: 1
  Change condition bitmask: 0x0 Action-id-bitmask: 0x0
  Signal bitmask: 0x0           Last signal bitmask: 0x0
  Details: Bearer trigger, Offline RG
  Collection time: None collected
```


CHAPTER 32

Charging Operational Commands

clear unified-edge ggsn-pgw charging cdr

Syntax	clear unified-edge ggsn-pgw charging cdr gateway-name <i>name</i> <transport-profile-name <i>profile-name</i>>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Clear the Charging Data Records (CDRs) from the services PICs for the configured transport profiles on the specified gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW).
Options	gateway-name <i>name</i> —Clear CDRs from the services PICs for the specified GGSN or P-GW. transport-profile-name <i>profile-name</i> —(Optional) Clear CDRs from the services PICs only for the specified transport profile.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show unified-edge ggsn-pgw charging transfer status on page 1143
List of Sample Output	clear unified-edge ggsn-pgw charging cdr gateway-name <i>name</i> on page 1110
Output Fields	No message is displayed on successful execution of this command; otherwise an error message is displayed.

Sample Output

```
clear unified-edge  user@host> clear unified-edge ggsn-pgw charging cdr gateway-name PGW
ggsn-pgw charging cdr
gateway-name name
```

clear unified-edge ggsn-pgw charging cdr wfa

Syntax	<code>clear unified-edge ggsn-pgw charging cdr wfa gateway-name <i>name</i> <transport-profile-name <i>profile-name</i>></code>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Clear from the services PICs the Charging Data Records (CDRs) that have not received an acknowledgement from the charging gateway function (CGF), the Routing Engine, or both.
Options	<p>gateway-name <i>name</i>—Clear the unacknowledged CDRs from the services PICs for the specified GGSN or P-GW.</p> <p>transport-profile-name <i>profile-name</i>—(Optional) Clear the unacknowledged CDRs from the services PICs only for the specified transport profile.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show unified-edge ggsn-pgw charging transfer status on page 1143
List of Sample Output	clear unified-edge ggsn-pgw charging cdr wfa gateway-name <i>name</i> on page 1111
Output Fields	No message is displayed on successful execution of this command; otherwise an error message is displayed.

Sample Output

```
clear unified-edge user@host> clear unified-edge ggsn-pgw charging cdr wfa gateway-name PGW
ggsn-pgw charging cdr
wfa gateway-name
name
```

clear unified-edge ggsn-pgw charging local-persistent-storage statistics

Syntax	clear unified-edge ggsn-pgw charging local-persistent-storage statistics <gateway-name <i>name</i> >
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Clear the storage statistics of the Charging Data Record (CDR) files on the local Routing Engine disk on one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then storage statistics for all GGSNs or P-GWs are cleared.
Options	gateway-name <i>name</i> —(Optional) Clear the storage statistics for the specified gateway.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show unified-edge ggsn-pgw charging local-persistent-storage statistics on page 1123
List of Sample Output	clear unified-edge ggsn-pgw charging local-persistent-storage statistics gateway-name <i>name</i> on page 1112
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear unified-edge	user@host> clear unified-edge ggsn-pgw charging local-persistent-storage statistics
ggsn-pgw charging	gateway-name PGW
local-persistent-storage	Cleared charging local persistent storage statistics
statistics	
gateway-name <i>name</i>	

clear unified-edge ggsn-pgw charging path statistics

Syntax	clear unified-edge ggsn-pgw charging path statistics gateway-name <i>name</i> <fpc-slot <i>slot-number</i> pic-slot <i>slot-number</i> > <gtpp-peer-addr <i>ipv4-address</i> > <gtpp-peer-name <i>peer-name</i> >
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Clear the path management message statistics between the charging data function (CDF) and the charging gateway function (CGF) servers for the specified gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW).
Options	<p>gateway-name <i>name</i>—Clear the path management message statistics for the specified GGSN or P-GW.</p> <p>fpc-slot <i>slot-number</i> pic-slot <i>slot-number</i>—(Optional) Clear the path management message statistics only for the specified FPC slot number and PIC slot number.</p> <p>gtpp-peer-addr <i>ipv4-address</i>—(Optional) Clear the path management message statistics only for the GTP Prime peer with the specified IPv4 address.</p> <p>gtpp-peer-name <i>peer-name</i>—(Optional) Clear the path management message statistics only for the GTP Prime peer with the specified name.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show unified-edge ggsn-pgw charging path statistics on page 1128
List of Sample Output	clear unified-edge ggsn-pgw charging path statistics gateway-name <i>name</i> on page 1113
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
clear unified-edge      user@host> clear unified-edge ggsn-pgw charging path statistics gateway-name PGW
ggsn-pgw charging      Cleared charging path statistics
path statistics
gateway-name name
```

clear unified-edge ggsn-pgw charging transfer statistics

Syntax	<code>clear unified-edge ggsn-pgw charging transfer statistics gateway-name <i>name</i></code> <code><fpc-slot <i>slot-number</i> pic-slot <i>slot-number</i>></code> <code><transport-profile-name <i>profile-name</i>></code>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Clear the charging transfer statistics on one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then charging transfer statistics for all GGSNs or P-GWs are cleared.
Options	<p>gateway-name <i>name</i>—Clear the transfer statistics for the specified GGSN or P-GW.</p> <p>fpc-slot <i>slot-number</i> pic-slot <i>slot-number</i>—(Optional) Clear the transfer statistics for the configured transport profiles for the specified FPC slot number and PIC slot number.</p> <p>transport-profile-name <i>profile-name</i>—(Optional) Clear the transfer statistics only for the specified transport profile.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show unified-edge ggsn-pgw charging transfer statistics on page 1139
List of Sample Output	clear unified-edge ggsn-pgw charging transfer statistics gateway-name name on page 1114
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

<code>clear unified-edge ggsn-pgw charging transfer statistics gateway-name name</code>	<code>user@host> clear unified-edge ggsn-pgw charging transfer statistics gateway-name PGW</code> Cleared charging transfer statistics
---	--

clear unified-edge sgw charging cdr

Syntax	clear unified-edge sgw charging cdr <gateway-name <i>name</i> > <transport-profile-name <i>profile-name</i> >
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Clear the Charging Data Records (CDRs) from the services PICs for the configured transport profiles on one or more Serving Gateways (S-GWs). If a gateway name is not specified, then the CDRs from the services PICs for all the S-GWs are cleared.
Options	<p>none—Clear the CDRs from the services PICs on all S-GWs.</p> <p>gateway-name <i>name</i>—(Optional) Clear the CDRs from the services PICs for the specified gateway.</p> <p>transport-profile-name <i>profile-name</i>—(Optional) Clear the CDRs from the services PICs for the specified transport profile.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show unified-edge sgw charging transfer status on page 1168
List of Sample Output	clear unified-edge sgw charging cdr gateway-name SGW on page 1115
Output Fields	No message is displayed on successful execution of this command; otherwise an error message is displayed.

Sample Output

```
clear unified-edge sgw      user@host> clear unified-edge sgw charging cdr gateway-name SGW
charging cdr
gateway-name SGW
```

clear unified-edge sgw charging local-persistent-storage statistics

Syntax	clear unified-edge sgw charging local-persistent-storage statistics <gateway-name <i>name</i>>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Clear the storage statistics of the Charging Data Record (CDR) files on the local Routing Engine disk on one or more Serving Gateways (S-GWs). If a gateway name is not specified, then storage statistics for all S-GWs are cleared.
Options	gateway-name <i>name</i> —(Optional) Clear the storage statistics for the specified gateway.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show unified-edge sgw charging local-persistent-storage statistics on page 1148
List of Sample Output	clear unified-edge sgw charging local-persistent-storage statistics on page 1116
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear unified-edge sgw charging local-persistent-storage statistics	user@host> clear unified-edge sgw charging local-persistent-storage statistics Cleared charging local persistent storage statistics
--	--

clear unified-edge sgw charging path statistics

Syntax	<pre>clear unified-edge sgw charging path statistics <fpc-slot slot-number> <gateway-name name> <gtp-peer-addr ipv4-address> <gtp-peer-name peer-name> <pic-slot slot-number></pre>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Clear the path management message statistics (between the charging data function [CDF] and the charging gateway function [CGF] servers) on one or more Serving Gateways (S-GWs). If a gateway name is not specified, then the path management statistics for all S-GWs are cleared.
Options	<p>fpc-slot <i>slot-number</i>—(Optional) Clear the path management message statistics for the specified FPC slot number.</p> <p>gateway-name <i>name</i>—(Optional) Clear the path management message statistics for the specified gateway.</p> <p>gtp-peer-addr <i>ipv4-address</i>—(Optional) Clear the path management message statistics for the GTP Prime peer with the specified IPv4 address.</p> <p>gtp-peer-name <i>peer-name</i>—(Optional) Clear the path management message statistics for the GTP Prime peer with the specified name.</p> <p>pic-slot <i>slot-number</i>—(Optional) Clear the path management message statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show unified-edge sgw charging path statistics on page 1154
List of Sample Output	clear unified-edge sgw charging path statistics on page 1117
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
clear unified-edge sgw charging path statistics
user@host> clear unified-edge sgw charging path statistics
Cleared charging path statistics
```

clear unified-edge sgw charging transfer statistics

Syntax	<code>clear unified-edge sgw charging transfer statistics</code> <code><fpc-slot slot-number></code> <code><gateway-name name></code> <code><pic-slot slot-number></code> <code><transport-profile-name profile-name></code>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Clear the transfer statistics on one or more Serving Gateways (S-GWs). If a gateway name is not specified, then the transfer statistics for all S-GWs are cleared.
Options	<p>none—Clear the transfer statistics for all S-GWs.</p> <p>fpc-slot slot-number—(Optional) Clear the transfer statistics for the specified FPC slot number.</p> <p>gateway-name name—(Optional) Clear the transfer statistics for the specified gateway.</p> <p>pic-slot slot-number—(Optional) Clear the transfer statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.</p> <p>transport-profile-name profile-name—(Optional) Clear the transfer statistics for the specified transport profile.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show unified-edge sgw charging transfer statistics on page 1164
List of Sample Output	clear unified-edge sgw charging transfer statistics on page 1118
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

<code>clear unified-edge sgw charging transfer statistics</code>	<code>user@host> clear unified-edge sgw charging transfer statistics</code> Cleared charging transfer statistics
--	--

request system storage unified-edge charging media start

Syntax	request system storage unified-edge charging media start <re0 re1>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Enable use of local persistent storage for Charging Data Records (CDRs).
Options	re0 re1 —(Optional) On routers that support dual or redundant Routing Engines, use the disk on the Routing Engine in slot 0 (re0) or Routing Engine in slot 1 (re1).
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • request system storage unified-edge media prepare on page 1122 • request system storage unified-edge charging media stop on page 1120 • show unified-edge ggsn-pgw charging local-persistent-storage statistics on page 1123
List of Sample Output	request system storage unified-edge charging media start on page 1119
Output Fields	When you enter this command, there is no output for success but an error displays if the command fails to complete.

Sample Output

```
request system user@host> request system storage unified-edge charging media start
storage unified-edge
charging media start
```

[request system storage unified-edge charging media stop](#)

Syntax	<code>request system storage unified-edge charging media stop <re0 re1></code>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Disable use of local persistent storage for Charging Data Records (CDRs).
Options	re0 re1 —(Optional) On routers that support dual or redundant Routing Engines, use the disk on the Routing Engine in slot 0 (re0) or Routing Engine in slot 1 (re1).
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system storage unified-edge media eject on page 1121• request system storage unified-edge charging media start on page 1119
List of Sample Output	request system storage unified-edge charging media stop on page 1120
Output Fields	When you enter this command, there is no output for success but an error displays if the command fails to complete.

Sample Output

<code>request system storage unified-edge charging media stop</code>	<code>user@host> request system storage unified-edge charging media stop</code>
--	--

request system storage unified-edge media eject

Syntax	request system storage unified-edge media eject <re0 re1>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Prepare the Solid State Disk (SSD) for removal from the Routing Engine. This command unmounts the SSD from /opt/mobility .
Options	re0 re1 —(Optional) On routers that support dual or redundant Routing Engines, prepare the disk on the Routing Engine in slot 0 (re0) or Routing Engine in slot 1 (re1).
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • request system storage unified-edge charging media stop on page 1120
List of Sample Output	request system storage unified-edge media eject on page 1121
Output Fields	When you enter this command, you are provided feedback on the status of your request.


Sample Output

```

request system      user@host> request system storage unified-edge media eject
storage unified-edge Media successfully ejected
media eject

```

request system storage unified-edge media prepare

Syntax	<code>request system storage unified-edge media prepare</code> <code><no-format></code> <code><re0 re1></code>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Prepare the Solid State Disk (SSD) on the Routing Engine for local persistent storage of Charging Data Records (CDRs). This command formats the SSD and mounts it to <code>/opt/mobility</code> .
	<div> NOTE: If you do not want to format the existing content on the SSD, you must specify the <code>no-format</code> option.</div>
Options	<p>no-format—(Optional) Do not format the existing content on the SSD when preparing the disk on the Routing Engine.</p> <p>re0 re1—(Optional) On routers that support dual or redundant Routing Engines, prepare the disk on the Routing Engine in slot 0 (re0) or Routing Engine in slot 1 (re1).</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• request system storage unified-edge charging media start on page 1119• show unified-edge ggsn-pgw charging local-persistent-storage statistics on page 1123
List of Sample Output	request system storage unified-edge media prepare on page 1122
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system storage unified-edge media prepare	<pre>user@host> request system storage unified-edge media prepare Creating filesystem Mounting media Media successfully prepared</pre>
--	---

show unified-edge ggsn-pgw charging local-persistent-storage statistics

Syntax	show unified-edge ggsn-pgw charging local-persistent-storage statistics <gateway gateway>
Release Information	Command introduced in Junos OS Mobility Release 11.2W. gateway-name option introduced in Junos OS Mobility Release 11.4W.
Description	Display the storage statistics of the Charging Data Record (CDR) files on the local Routing Engine disk for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then the status for all GGSNs and P-GWs is displayed.
Options	gateway gateway-name —(Optional) Display the storage statistics for the specified GGSN or P-GW.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear unified-edge ggsn-pgw charging local-persistent-storage statistics on page 1112
List of Sample Output	show unified-edge ggsn-pgw charging local-persistent-storage statistics on page 1127
Output Fields	Table 77 on page 1123 lists the output fields for the show unified-edge ggsn-pgw charging local-persistent-storage statistics command. Output fields are listed in the approximate order in which they appear.

Table 77: show unified-edge ggsn-pgw charging local-persistent-storage statistics Output Fields

Field Name	Field Description
Batch Messages received	Total number of batch messages sent from services PICs to the Routing Engine disk. The CDRs generated in services PICs are sent to the local Routing Engine disk as batch messages.
Batch Responses sent	Total number of responses sent for the received batch messages.
Invalid Messages received	Total number of invalid batch messages sent from services PICs to the Routing Engine disk.
Number of temp log files opened	Total number of temporary CDR files opened on the Routing Engine disk. These files are closed and copied from the temporary location to a final location (/opt/mobility/charging/ggsn/final_log) within the same Routing Engine disk, from where they can be transferred using SSH FTP (SFTP). A file is closed when the file size, file age, or the maximum number of CDRs added to the file reaches the configured limit (or the default limit, when no limit is configured).

Table 77: show unified-edge ggsn-pgw charging local-persistent-storage statistics Output Fields (continued)

Field Name	Field Description
Number of journal files opened	Total number of open journal files. Journal files are used to remove any unfinished file writes from the temporary log files if a daemon or router crash interrupts the kernel file write. When the daemon or router come back up, the journal log files are read to ensure that the contents of the temporary log file are sane. If there is any unfinished CDR data, the temporary log file is truncated to the last-known successful file write. For each temporary log CDR file, a separate journal file is opened.
Number of journal files closed	Total number of journal files closed.
Number of CDR log files closed	Total number of temporary CDR log files closed. Authorized users can use SFTP to transfer these files from the <code>/opt/mobility/charging/ggsn/final_log</code> location.
Number of CDR files closed due to file-age	Total number of temporary CDR log files closed because the age of the files reached the configured limit (or the default limit, when no limit is configured). The default value for the file age is 120 minutes.
Number of CDR files closed due to file-size	Total number of number of temporary CDR log files closed because the size of the files reached the configured limit (or the default limit, when no limit is configured). The default file size is 10 MB.
Number of CDR files closed due to cdr-count	Total number of temporary CDR log files closed because the maximum number of CDRs added to the files reached the configured limit. There is no default limit.
Abnormal file closures	Total number of abnormal temporary CDR log file closures. This counter is incremented when the charging daemon comes up after a system reboot or crash and temporary CDR log file closures are triggered.
Normal file closures	Total number of normal temporary CDR log file closures. This counter is incremented when changes in the configuration, such as a file format change, trigger temporary CDR log file closures.
Number of CDR log files closed in TS_32_297 format	Total number of closed temporary CDR log files that are compliant with the format specified in the 32297 technical specification release.
Number of CDR log files closed in raw asnl format	Total number of closed temporary CDR log files that are in the raw ASN.1 format.
Total number of CDRs backed up	Total number of CDRs backed up to the standby Routing Engine.

Table 77: show unified-edge ggsn-pgw charging local-persistent-storage statistics Output Fields (*continued*)

Field Name	Field Description
Disk Full messages sent	<p>Total number of messages sent by the Routing Engine to the services PICs to indicate that its disk is full and unable to accept any more charging data.</p> <p>You can use SFTP to transfer the files from the <code>/opt/mobility/charging/ggsn/final_log</code> location to free disk space, or remove the disk and copy the files.</p> <p>You can remove the disk by issuing the following commands in this order:</p> <ul style="list-style-type: none"> • request system storage unified-edge charging media stop • request system storage unified-edge media eject
Disk Full resolve messages sent	<p>Total number of disk full resolve messages sent. When the disk space is freed, the Routing Engine sends messages to the services PICs indicating that it can receive charging data.</p>
Number of async IO reqs written	<p>Number of asynchronous I/O requests written. This counter is incremented once for every write operation into the temporary log CDR file.</p>
Disk space status	<p>Indicates whether disk space is available for storage. The possible values are:</p> <ul style="list-style-type: none"> • DISK_AVAILABLE • DISK_AT_WATERMARK_LEVEL1 • DISK_AT_WATERMARK_LEVEL2 • DISK_AT_WATERMARK_LEVEL3 • DISK_OFFLINE—Indicates that a disk is not present or the request system storage unified-edge charging media stop command has been issued. • DISK_OFFLINE_PENDING—Indicates whether any CDRs are being written or mirrored on the backup Routing Engine. This interim status message is displayed after the request system storage unified-edge charging media stop command has been issued but before the disk goes offline.
Watermark level1 at (MB)	<p>Indicates the percentage of the total Routing Engine disk space configured for storage. By default, watermark level 1 is set to 70 percent of the total disk space.</p> <p>When this limit is reached, an alert (if configured) is sent and you can take corrective measures to free the disk space.</p>
Watermark level2 at (MB)	<p>Indicates the percentage of the total Routing Engine disk space configured for storage. By default, watermark level 2 is set to 80 percent of the total disk space.</p> <p>When this limit is reached, an alert (if configured) is sent and you can take corrective measures to free the disk space.</p>
Watermark level3 at (MB)	<p>Indicates the percentage of the total Routing Engine disk space configured for storage. By default, watermark level 3 is set to 90 percent of the total disk space.</p> <p>When this limit is reached, an alert (if configured) is sent and you can take corrective measures to free the disk space. If an alert is not configured, the services PICs stop sending the charging data to the Routing Engine disk and you must transfer the files using SFTP to free the disk space. However, this data is not lost because it is buffered in the services PICs. The services PICs can buffer up to a maximum of 2 GB of data, after which a Call Admission Control (CAC) is triggered.</p>

Table 77: show unified-edge ggsn-pgw charging local-persistent-storage statistics Output Fields (*continued*)

Field Name	Field Description
Temporary CDR log file Statistics —The following information for the temporary CDR log files is displayed only if temporary CDR log files are currently open.	
File Name	Name of the temporary CDR log file.
Journal file name	Name of the journal file.
Current number of CDRs	Total number of CDRs that have been currently added to the temporary CDR log file.
Current file size (bytes)	Current size, in bytes, of the temporary CDR log file.
File age trigger (mins)	Configured duration, in minutes, after which the temporary CDR log file is closed. If this parameter is not configured, then the default value is displayed.
File size trigger (bytes)	Configured size, in bytes, that the temporary CDR log file can reach after which it is closed. If this parameter is not configured, then the default value is displayed.
CDR count trigger	Configured maximum number of CDRs that can be added to the temporary CDR log file, after which it is closed. If this parameter is not configured, then the default value is displayed.
Global Statistics	
Disk Offline messages sent	<p>Total number of messages sent by the Routing Engine to the services PICs to indicate that its disk is offline or is not mounted, and that it is unable to accept any more charging data.</p> <p>You can configure the disk (storage media) to store charging data by issuing these commands:</p> <ul style="list-style-type: none"> request system storage unified-edge media prepare request system storage unified-edge charging media start
Disk Available messages sent	When the disk is prepared and mounted, the Routing Engine sends messages to the services PICs to indicate that it can now receive charging data. This field indicates the total number of these messages sent.
Number of CDR storage files on disk	Total number of CDR files stored on the local Routing Engine disk.
Current storage space in use (MB)	Storage space, in MB, that is currently being used.
Available storage space on disk (MB)	Total free space, in MB, available for storage on the disk.
Total storage space on disk (MB)	Total storage space, in MB, on the disk.

Sample Output

```

show unified-edge      user@host> show unified-edge ggsn-pgw charging local-persistent-storage statistics
ggsn-pgw charging      Gateway: PGW
local-persistent-storage Charging Local-persistent-storage Statistics
statistics              Batch Messages received           : 46
                        Batch Responses sent           : 46
                        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    : 949
                        Disk Full messages sent          : 0
                        Disk Full resolve messages sent   : 0
                        Number of async IO reqs written   : 46
                        Disk space status                : DISK_AVAILABLE
                        Watermark level1 at(MB)           : 618(70%)
                        Watermark level2 at(MB)           : 706(80%)
                        Watermark level3 at(MB)           : 794(90%)

Temporary CDR log file Statistics
File Name: /opt/mobility/charging/ggsn/temp_log/templog_file_1.log
Journal file name      : /opt/mobility/charging/ggsn/jrn1/jrn1_1.log
Current number of CDRs : 949
Current file size(bytes) : 288642
File age trigger(mins) : 60
File size trigger(bytes) : 10485760
CDR count trigger      : 0

Global Statistics
Disk Offline messages sent : 0
Disk Available messages sent : 0
Number of CDR storage files on disk : 0
Current storage space in use(MB) : 301
Available storage space on disk(MB) : 582
Total storage space on disk(MB) : 883

```

show unified-edge ggsn-pgw charging path statistics

Syntax	show unified-edge ggsn-pgw charging path statistics <brief detail> <fpc-slot <i>slot-number</i> pic-slot <i>slot-number</i>> <gateway <i>gateway-name</i>> <gtp-peer-addr <i>ipv4-address</i>> <gtp-peer-name <i>peer-name</i>>
Release Information	Command introduced in Junos OS Mobility Release 11.2W. gateway-name option introduced in Junos OS Mobility Release 11.4W.
Description	Display the path management message statistics (between the Charging Data Function (CDF) and the Charging Gateway Function (CGF) servers) for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then the statistics for all GGSNs and P-GWs is displayed.
Options	none —(Same as brief) Display the path management message statistics. brief detail —(Optional) Display the specified level of output. The brief option displays the statistics per GGSN or P-GW for all services PICs. The detail option displays the statistics per GGSN or P-GW for each services PIC. fpc-slot <i>slot-number</i> pic-slot <i>slot-number</i> —(Optional) Display the path management message statistics only for the specified Flexible PIC Concentrator (FPC) slot number and PIC slot number. gateway <i>gateway-name</i> —(Optional) Display the path management statistics for the specified GGSN or P-GW. gtp-peer-addr <i>ipv4-address</i> —(Optional) Display the path management message statistics only for the GPRS tunneling protocol Prime (GTP Prime) peer with the specified IPv4 address. gtp-peer-name <i>peer-name</i> —(Optional) Display the path management message statistics only for the GTP Prime peer with the specified name.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• clear unified-edge ggsn-pgw charging path statistics on page 1113
List of Sample Output	show unified-edge ggsn-pgw charging path statistics brief on page 1131 show unified-edge ggsn-pgw charging path statistics detail on page 1131
Output Fields	Table 78 on page 1129 lists the output fields for the show unified-edge ggsn-pgw charging path statistics command. Output fields are listed in the approximate order in which they appear.

Table 78: show unified-edge ggsn-pgw charging path statistics Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the GGSN or P-GW.	All levels none
FPC/PIC	FPC slot number and PIC slot number for which the statistics are displayed.	detail
CGF Address	Address of the CGF server (GTP Prime peer).	All levels none
CGF Server Name	Name of the CGF server (GTP Prime peer).	All levels none
Echo Requests Rx	Total number of echo requests received by the CDF from the CGF sever.	All levels none
Echo Responses Tx	Total number of echo responses transmitted by the CDF to the CGF sever.	All levels none
Echo Responses Rx	Total number of echo responses received by the CDF from the CGF server.	All levels none
Echo Requests Tx	Total number of echo requests transmitted by the CDF to the CGF server.	All levels none
Node-Alive Requests Rx	Total number of node alive requests received by the CDF from the CGF server.	All levels none
Node-Alive Responses Tx	Total number of responses transmitted by the CDF to the node alive requests received from the CGF server.	All levels none
Version Not Supported Rx	Total number of Version Not Supported messages received by the CDF from the CGF server. The CGF server sends these messages to the CDF to indicate that the GTP Prime messages sent by the CDF are incompatible with the GTP Prime version supported by the CGF server.	All levels none
Version Not Supported Tx	Total number of Version Not Supported messages transmitted by the CDF to the CGF server. The CDF sends these messages to indicate that the GTP Prime messages sent by the CGF server are incompatible with the GTP Prime version supported by the CDF.	All levels none
Echo Requests timed out	Total number of echo requests sent by the CDF for which there were no responses from the CGF server and that have timed out.	All levels none

Table 78: show unified-edge ggsn-pgw charging path statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
Echo Interval	Configured echo interval, in seconds. If the echo interval is not configured, then the default value is displayed.	All levels none
Down Detection Interval	Configured down detect time, in seconds. If the down detect time is not configured, then the default value is displayed.	All levels none
Reconnect Time Interval	Configured reconnect time, in seconds. If the reconnect time is not configured, then the default value is displayed.	All levels none
Destination Port	Configured destination port. If the destination port is not configured, then the default port (3386) is displayed.	All levels none
Pending Queue Size	Configured pending queue size. If the pending queue size is not configured, then the default value (1024) is displayed.	All levels none
Path Manager FPC Slot	FPC slot that manages the path management messages.	All levels none
Path Manager PIC Slot	PIC slot that manages the path management messages.	All levels none
Path Manager Port	Port used for path management messages.	All levels none
T3 Response Time Interval	Configured T3 response time interval, in seconds. If the T3 response time is not configured, then the default value (5 seconds) is displayed.	All levels none
Source Interface Valid	Indicates whether the source interface is valid or not.	All levels none
GTPP Header Type	Configured header type for the GTP Prime messages.	All levels none
N3 Requests	Configured value for N3 requests . If the N3 requests value is not configured, then the default value (3) is displayed.	All levels none
Local Address	Address of the local loopback source interface from which the GTP Prime packets are sent to the CGF server.	All levels none

Table 78: show unified-edge ggsn-pgw charging path statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
GTPP Version	Configured version that is supported on the configured local loopback source interface's IP address, from which the GTP Prime packets are sent to the CGF server.	All levels none
Transport Protocol	Configured transport protocol for sending the GTP Prime packets from CDF to the CGF server.	All levels none
TCP Port Range Start	Start of the range of source ports from which the TCP connection from each services PIC to the CGF server can originate. The GGSN or P-GW assigns a range of source ports internally.	All levels none
TCP Port Range End	End of the range of source ports from which the TCP connection from each services PIC to the CGF server can originate. The GGSN or P-GW assigns a range of source ports internally.	All levels none
TCP Connection State	Indicates whether the TCP connection state on the services PIC has been established or not.	detail

Sample Output

**show unified-edge
ggsn-pgw charging
path statistics brief**

```
user@host> show unified-edge ggsn-pgw charging path statistics brief
Gateway: PGW
Charging Path Statistics
```

CGF Address	: 2.2.2.2	CGF Server Name	: p_cgf
Echo Requests	Rx: 0	Echo Responses	Tx: 0
Echo Responses	Rx: 0	Echo Requests	Tx: 0
Node-Alive Requests	Rx: 0	Node-Alive Responses	Tx: 0
Version Not Supported	Rx: 0	Version Not Supported	Tx: 0
Echo Requests timed out	: 0	Echo Interval	: 0
Down Detection Interval	: 10	Reconnect Time Interval	: 60
Destination Port	: 3386	Pending Queue Size	: 1000
Path Manager FPC Slot	: 5	Path Manager PIC Slot	: 0
T3 Response Time Interval	: 5	Path Manager Port	: 30275
Source Interface Valid	: Yes	GTPP Header Type	: long
N3 Requests	: 1	Local Address	: 12.4.1.1
GTPP Version	: V0	Transport Protocol	: TCP
TCP Port Range Start	: 30277	TCP Port Range End	: 30308


**show unified-edge
ggsn-pgw charging
path statistics detail**

```
user@host> show unified-edge ggsn-pgw charging path statistics detail
Gateway: PGW
Charging Path Statistics
FPC/PIC: 5/0
```

CGF Address	: 2.2.2.2	CGF Server Name	: p_cgf
Echo Requests	Rx: 0	Echo Responses	Tx: 0
Echo Responses	Rx: 0	Echo Requests	Tx: 0
Node-Alive Requests	Rx: 0	Node-Alive Responses	Tx: 0
Version Not Supported	Rx: 0	Version Not Supported	Tx: 0
Echo Requests timed out	: 0	Echo Interval	: 0

Down Detection Interval	: 10	Reconnect Time Interval	: 60
Destination Port	: 3386	Pending Queue Size	: 1000
Path Manager FPC Slot	: 5	Path Manager PIC Slot	: 0
T3 Response Time Interval	: 5	Path Manager Port	: 30275
Source Interface Valid	: Yes	GTPP Header Type	: long
N3 Requests	: 1	Local Address	: 12.4.1.1
GTPP Version	: V0	Transport Protocol	: TCP
TCP Port Range Start	: 30277	TCP Port Range End	: 30308
TCP Connection State	: Established		

show unified-edge ggsn-pgw charging path status

Syntax	<pre>show unified-edge ggsn-pgw charging path status <brief detail> <fpc-slot slot-number pic-slot slot-number> <gateway gateway-name> <gtp-peer-addr ipv4-address> <gtp-peer-name peer-name></pre>
Release Information	<p>Command introduced in Junos OS Mobility Release 11.2W.</p> <p>gateway-name option introduced in Junos OS Mobility Release 11.4W.</p>
Description	<p>Display the status of the configured GPRS tunneling protocol (GTP) Prime peers for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then the status for all GGSNs and P-GWs is displayed.</p> <p>The status includes information about whether the GTP Prime peers are connected, down, or still in the process of establishing a connection, and whether the echo messages are enabled or disabled.</p> <div style="margin-top: 20px;">  <p>NOTE: In charging, the terms GTP Prime peers and charging gateway function (CGF) server are used interchangeably.</p> </div>
Options	<p>none—(Same as brief) Display the status of the configured peers.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>fpc-slot slot-number pic-slot slot-number—(Optional) Display the status of the configured peers only for the specified FPC slot number and PIC slot number.</p> <p>gateway gateway-name—(Optional) Display the path management statistics for the specified GGSN or P-GW.</p> <p>gtp-peer-addr ipv4-address—(Optional) Display the status of the configured peers only for the GTP Prime peer with the specified IPv4 address.</p> <p>gtp-peer-name peer-name—(Optional) Display the status of the configured peers only for the GTP Prime peer with the specified name.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show unified-edge ggsn-pgw charging path statistics on page 1128
List of Sample Output	<p>show unified-edge ggsn-pgw charging path status on page 1134</p> <p>show unified-edge ggsn-pgw charging path status detail on page 1134</p>

Output Fields Table 79 on page 1134 lists the output fields for the **show unified-edge ggsn-pgw charging path status** command. Output fields are listed in the approximate order in which they appear.

Table 79: show unified-edge ggsn-pgw charging path status Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the GGSN or P-GW.	All levels none
Peer-Address	Address of the CGF server (GTP Prime peer).	All levels none
Peer-Name	Name of the CGF server (GTP Prime peer).	All levels none
Local-Address	IPv4 address of the local loopback source interface from where the GTP Prime packets are sent to the CGF server (GTP Prime peer).	All levels none
Status	Status of the CGF server: <ul style="list-style-type: none"> • Connected • Down • In-Progress 	All levels none
Echo	Indicates whether echo messages are enabled or disabled. The possible values are: <ul style="list-style-type: none"> • Enabled or Disabled for UDP connections • N/A (Not Applicable) for TCP connections 	All levels none
Cause	Probable cause for the current status of the CGF peer. This field is displayed only when the CGF server is down or the connection has not been established.	detail
FPC/PIC	FPC and PIC slot numbers.	detail

Sample Output

```

show unified-edge user@host> show unified-edge ggsn-pgw charging path status
ggsn-pgw charging
path status      Gateway: PGW
                  Charging Path Status
                  Peer-Address    Peer-Name    Local-Address    Status    Echo
                  2.2.2.2         p_cgf        12.4.1.1         Connected N/A

```

```

show unified-edge user@host> show unified-edge ggsn-pgw charging path status detail
ggsn-pgw charging
path status detail Gateway: PGW
                  Charging Path Status

```

```
FPC/PIC 5/0
Peer-Address 2.2.2.2
Peer-Name    p_cgf
Local-Address 12.4.1.1
Status       Connected
Echo         N/A
```

show unified-edge ggsn-pgw charging service-mode

Syntax	show unified-edge ggsn-pgw charging service-mode gateway <i>gateway-name</i> <brief detail> <charging-profile <i>profile-name</i>> <transport-profile <i>profile-name</i>>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Display the charging service mode information for the specified Gateway GPRS Support Node (GGSN) or Packet Data Network Gateway (P-GW).
Options	<p>gateway <i>gateway-name</i>—Display the charging service mode information for the specified GGSN or P-GW.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>charging-profile-name <i>profile-name</i>—(Optional) Display the service mode information for the specified charging profile.</p> <p>transport-profile-name <i>profile-name</i>—(Optional) Display the service mode information for the specified transport profile.</p>
Required Privilege Level	view
List of Sample Output	show unified-edge ggsn-pgw charging service-mode gateway PGW brief on page 1137 show unified-edge ggsn-pgw charging service-mode gateway PGW detail on page 1138
Output Fields	Table 80 on page 1136 lists the output fields for the show unified-edge ggsn-pgw charging service-mode command. Output fields are listed in the approximate order in which they appear.

Table 80: show unified-edge ggsn-pgw charging service-mode Output Fields

Field Name	Field Description	Level of Output
Gateway Name	Name of the GGSN or P-GW.	All levels

Table 80: show unified-edge ggsn-pgw charging service-mode Output Fields (*continued*)

Field Name	Field Description	Level of Output
Service Mode	Service mode for the gateway. The following service modes are possible: <ul style="list-style-type: none"> Maintenance—Gateway is in maintenance mode. MM Active Phase—In this mode, you can make changes to any of the configuration options under the [edit unified-edge gateways ggsn-pgw gateway-name charging charging-profiles] or the [edit unified-edge gateways ggsn-pgw gateway-name charging transport-profiles] hierarchy levels. MM In/Out Phase—In this mode, you cannot make changes to the configuration options under the [edit unified-edge gateways ggsn-pgw gateway-name charging charging-profiles] or the [edit unified-edge gateways ggsn-pgw gateway-name charging transport-profiles] hierarchy levels. Operational—Gateway is still in operational mode and not in maintenance mode. You can use the following commands to put the charging profile or transport profile in maintenance mode: <ul style="list-style-type: none"> set unified-edge gateways ggsn-pgw gateway-name charging charging-profiles profile-name service-mode maintenance set unified-edge gateways ggsn-pgw gateway-name charging transport-profiles profile-name service-mode maintenance 	All levels
Charging Profile(s) or Charging Profile	Name of the charging profile.	All levels
Service Mode	Service mode for the charging profile.	All levels
Transport Profile(s) or Transport Profile	Name of the transport profile.	brief
Service Mode	Service mode for the transport profile.	All levels
Pending Maintenance Mode Ready Ack	Lists the components or modules that are not yet ready to accept the configuration changes. Maintenance mode becomes active only after all the components or modules are ready to accept these changes.	detail

Sample Output

```

show unified-edge ggsn-pgw charging service-mode gateway PGW brief
user@host> show unified-edge ggsn-pgw charging service-mode gateway PGW brief
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      : PGW
Service Mode      : Operational

Charging Profile(s)      Service Mode
p_juniper               Operational
Transport Profile(s)     Service Mode

```

p_tsp

Operational

```

show unified-edge      user@host> show unified-edge ggsn-pgw charging service-mode gateway PGW detail
ggsn-pgw charging      Gateway Name      : PGW
service-mode gateway    Service Mode      : Operational
PGW detail              Charging Profile: p_juniper
                        Service Mode      : Operational
                        Transport Profile: p_tsp
                        Service Mode      : Operational
    
```


show unified-edge ggsn-pgw charging transfer statistics

Syntax	<pre>show unified-edge ggsn-pgw charging transfer statistics <brief detail> <fpc-slot slot-number pic-slot slot-number> <gateway gateway-name> <transport-profile-name profile-name></pre>
Release Information	<p>Command introduced in Junos OS Mobility Release 11.2W.</p> <p>gateway option introduced in Junos OS Mobility Release 11.4W.</p>
Description	Display the transfer statistics for the configured transport profiles on one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then statistics for all GGSNs and P-GWs are displayed.
Options	<p>none—(Same as brief) Display the transfer statistics for the configured transport profiles for all GGSNs or P-GWs.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>fpc-slot slot-number pic-slot slot-number—(Optional) Display the transfer statistics only for the specified FPC slot number and PIC slot number.</p> <p>gateway gateway-name—(Optional) Display the transfer statistics for the specified GGSN or P-GW.</p> <p>transport-profile-name profile-name—(Optional) Display the transfer statistics only for the specified transport profile .</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear unified-edge ggsn-pgw charging transfer statistics on page 1114
List of Sample Output	<p>show unified-edge ggsn-pgw charging transfer statistics brief on page 1141</p> <p>show unified-edge ggsn-pgw charging transfer statistics detail on page 1141</p>
Output Fields	<p>Table 81 on page 1139 lists the output fields for the show unified-edge ggsn-pgw charging transfer statistics command. Output fields are listed in the approximate order in which they appear.</p>

Table 81: show unified-edge ggsn-pgw charging transfer statistics Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the GGSN or P-GW	All levels
		none
Transport-Profile	Name of the transport profile.	All levels
		none

Table 81: show unified-edge ggsn-pgw charging transfer statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
Redirection Requests Rx	<p>Total number of redirection request messages received by the charging data function (CDF) from the charging gateway function (CGF) server.</p> <p>The CGF server can send these messages to inform CDF about the following:</p> <ul style="list-style-type: none"> • The CGF server is about to stop service (possibly due to an error condition or for maintenance). • The next node in the chain (such as a billing server) has lost its connection to the CGF server. 	<p>All levels</p> <p>none</p>
Redirection Responses Tx	Total number of redirection response messages transmitted as responses to the redirection requests received. Redirection response messages indicate whether a redirection request message was successful or not.	<p>All levels</p> <p>none</p>
DRT Responses Rx	Total number of DRT response messages received for the Data Record Transfer (DRT) request messages sent. DRT response messages indicate whether a DRT request was successful or not.	<p>All levels</p> <p>none</p>
DRT Requests Tx	Total number of DRT request messages transmitted to the CGF server. These messages are used to transfer CDRs from the CDF to the CGF server.	<p>All levels</p> <p>none</p>
DRT successful Responses Rx	Total number of successful DRT response messages received for the DRT request messages sent.	<p>All levels</p> <p>none</p>
DRT Error Responses Rx	Total number of DRT error response messages received for the DRT request messages sent.	<p>All levels</p> <p>none</p>
DRT Requests timed out	Total number of DRT requests sent that timed out before receiving any responses from the CGF server.	<p>All levels</p> <p>none</p>
CGF Switch Back Times	Total number of times the CGF servers were switched, which indicates the number of times that the CGF servers were either offline or down for maintenance.	<p>All levels</p> <p>none</p>
Batch Requests Tx	Total number of batch requests transmitted (from services PICs) for a transport profile.	<p>All levels</p> <p>none</p>
Batch Response Errors Rx	Total number of error responses sent by the Routing Engine to the services PICs for the batch requests messages received.	<p>All levels</p> <p>none</p>
Batch CDR's Tx	Total number of CDRs transmitted from services PICs to the Routing Engine.	<p>All levels</p> <p>none</p>
CDR Count	Total number of CDRs transmitted to the CGF server.	<p>All levels</p> <p>none</p>

Table 81: show unified-edge ggsn-pgw charging transfer statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
Total WFA	Total number of request messages awaiting acknowledgements from either the Routing Engine or the CGF server.	All levels none
FPC/PIC	FPC and PIC slot numbers.	detail

Sample Output

```

show unified-edge user@host> show unified-edge ggsn-pgw charging transfer statistics brief
ggsn-pgw charging
transfer statistics brief
Gateway: PGW
Charging Transfer Statistics
Transport-Profile : p_tsp
  Redirection Requests    Rx: 1    Redirection Responses    Tx: 0
  DRT Responses           Rx: 0    DRT Requests             Tx: 2
  DRT successful Responses Rx: 0    DRT Error Responses      Rx: 0
  DRT Requests timed out  : 0    CGF Switch Back Times    : 0
  Batch Requests          Tx: 0    Batch Response Errors    Rx: 0
  Batch CDR's             Tx: 0    CDR Count                : 2
  Total WFA               : 0

[...output truncated]

Gateway: PGW2
Charging Transfer Statistics
Transport-Profile : p_tsp
  Redirection Requests    Rx: 1    Redirection Responses    Tx: 0
  DRT Responses           Rx: 0    DRT Requests             Tx: 5
  DRT successful Responses Rx: 0    DRT Error Responses      Rx: 0
  DRT Requests timed out  : 0    CGF Switch Back Times    : 1
  Batch Requests          Tx: 0    Batch Response Errors    Rx: 0
  Batch CDR's             Tx: 0    CDR Count                : 10
  Total WFA               : 0

[...output truncated...]

show unified-edge user@host> show unified-edge ggsn-pgw charging transfer statistics detail
ggsn-pgw charging
transfer statistics
detail
Gateway: PGW
Charging Transfer Statistics
FPC/PIC: 2/0
Transport-profile : p_tsp
  Redirection Requests    Rx: 1    Redirection Responses    Tx: 0
  DRT Responses           Rx: 0    DRT Requests             Tx: 2
  DRT successful Responses Rx: 0    DRT Error Responses      Rx: 0
  DRT Requests timed out  : 0    CGF Switch Back Times    : 0
  Batch Requests          Tx: 0    Batch Response Errors    Rx: 0
  Batch CDR's             Tx: 0    CDR Count                : 2
  Total WFA               : 0

[...output truncated...]

Gateway: PGW2
Charging Transfer Statistics
FPC/PIC: 2/1
Transport-profile : p_tsp

```

Redirection Requests	Rx: 1	Redirection Responses	Tx: 0
DRT Responses	Rx: 0	DRT Requests	Tx: 5
DRT successful Responses	Rx: 0	DRT Error Responses	Rx: 0
DRT Requests timed out	: 0	CGF Switch Back Times	: 1
Batch Requests	Tx: 0	Batch Response Errors	Rx: 0
Batch CDR's	Tx: 0	CDR Count	: 10
Total WFA	: 0		

[..output truncated...]

show unified-edge ggsn-pgw charging transfer status

Syntax	<pre>show unified-edge ggsn-pgw charging transfer status <brief detail> <fpc-slot slot-number pic-slot slot-number> <gateway gateway-name> <transport-profile-name profile-name></pre>
Release Information	<p>Command introduced in Junos OS Mobility Release 11.2W.</p> <p>gateway option introduced in Junos OS Mobility Release 11.4W.</p>
Description	<p>Display the Charging Data Record (CDR) transfer status for the configured transport profiles for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then the status for all GGSNs and P-GWs is displayed.</p>
Options	<p>none—(Same as brief) Display the total number of unacknowledged and buffered CDRs for the configured transport profiles for all GGSNs or P-GWs.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>fpc-slot slot-number pic-slot slot-number—(Optional) Display the total number of unacknowledged and buffered CDRs only for the specified FPC slot number and PIC slot number.</p> <p>gateway gateway-name—(Optional) Display the total number of unacknowledged and buffered CDRs for the configured transport profiles for the specified GGSN or P-GW.</p> <p>transport-profile-name profile-name—(Optional) Display the total number of unacknowledged and buffered CDRs only for the specified transport profile.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show unified-edge ggsn-pgw charging transfer statistics on page 1139
List of Sample Output	<p>show unified-edge ggsn-pgw charging transfer status on page 1144</p> <p>show unified-edge ggsn-pgw charging transfer status detail on page 1144</p>
Output Fields	<p>Table 82 on page 1143 lists the output fields for the show unified-edge ggsn-pgw charging transfer status command. Output fields are listed in the approximate order in which they appear.</p>

Table 82: show unified-edge ggsn-pgw charging transfer status Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the GGSN or P-GW	All levels
		none

Table 82: show unified-edge ggsn-pgw charging transfer status Output Fields (*continued*)

Field Name	Field Description	Level of Output
FPC/PIC	FPC and PIC slot numbers.	detail
Transport-Profile	Name of the transport profile.	All levels none
Transport-profile Id	ID of the transport profile.	detail
Total UnAck CDR's	Total number of CDRs (for the transport profile) sent to the charging gateway function (CGF) servers for which no acknowledgements were received.	All levels none
Total Buffered CDR's	Total number of buffered CDRs (for the transport profile) in the services PICs.	All levels none

Sample Output

```

show unified-edge user@host> show unified-edge ggsn-pgw charging transfer status
ggsn-pgw charging Gateway: PGW
transfer status   Charging Transfer Status
                  Transport-Profile : p_tsp
                  Total UnAck CDR's   : 2
                  Total Buffered CDR's : 0

                  Transport-Profile : 2
                  Total UnAck CDR's   : 0
                  Total Buffered CDR's : 0

                  Gateway: PGW2
                  Charging Transfer Status
                  Transport-Profile : p_tsp
                  Total UnAck CDR's   : 5
                  Total Buffered CDR's : 0

                  Transport-Profile : 2
                  Total UnAck CDR's   : 0
                  Total Buffered CDR's : 0

show unified-edge user@host> show unified-edge ggsn-pgw charging transfer status detail
ggsn-pgw charging Gateway: PGW
transfer status detail Charging Transfer Status
                    FPC/PIC: 2/0
                    Transport-profile      : p_tsp
                    Transport-profile Id    : 3
                    Total UnAck CDR's      : 2
                    Total Buffered CDR's    : 0

                    Transport-profile      : 2
                    Transport-profile Id    : 1
                    Total UnAck CDR's      : 0
                    Total Buffered CDR's    : 0

```

```
Gateway: PGW2
Charging Transfer Status
  FPC/PIC: 2/1
  Transport-profile      : p_tsp
  Transport-profile Id   : 6
  Total UnAck CDR's     : 5
  Total Buffered CDR's   : 0

  Transport-profile      : 2
  Transport-profile Id   : 4
  Total UnAck CDR's     : 0
  Total Buffered CDR's   : 0
```

show unified-edge ggsn-pgw charging trigger-profile

Syntax	show unified-edge ggsn-pgw charging trigger-profile <trigger-profile-name <i>profile-name</i>>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Display the configuration of the trigger profiles for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then information for all GGSNs and P-GWs is displayed.
Options	<p>none—(Same as brief) Display the configuration of the trigger profiles.</p> <p>trigger-profile-name <i>profile-name</i>—(Optional) Display the configuration only for the specified trigger profile.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • trigger-profiles on page 846
List of Sample Output	show unified-edge ggsn-pgw charging trigger-profile on page 1147
Output Fields	Table 83 on page 1146 lists the output fields for the show unified-edge ggsn-pgw charging trigger-profile command. Output fields are listed in the approximate order in which they appear.

Table 83: show unified-edge ggsn-pgw charging trigger-profile Output Fields

Field Name	Field Description	Level of Output
Profile Name	Name of the trigger profile.	All levels
		none
Profile ID	ID of the trigger profile.	All levels
		none
Time Limit	Time limit for the trigger profile, if any.	All levels
		none
Volume Limit	Volume limit for the trigger profile, if any.	All levels
		none
PLMN change trigger	<p>Indicates whether the Public Land Mobile Network (PLMN) change trigger is enabled or not.</p> <p>If this trigger is enabled, a PLMN change usually results in the CDR being updated with the charging information and then closed.</p>	All levels
		none

Table 83: show unified-edge ggsn-pgw charging trigger-profile Output Fields (*continued*)

Field Name	Field Description	Level of Output
QoS change trigger	Indicates whether the quality-of-service (QoS) change trigger is enabled or not.	All levels
	If this trigger is enabled, a QoS change usually results in a container being added to the CDR.	none
RAT change trigger	Indicates whether the Radio Access Technology (RAT) change trigger is enabled or not.	All levels
	If this trigger is enabled, a RAT change usually results in the CDR being updated with the charging information and then closed.	none
User location change trigger	Indicates whether the user-location change trigger is enabled or not.	All levels
	If this trigger is enabled, a user location change usually results in the current container being closed and added to the CDR.	none
MS Timezone change trigger	Indicates whether the mobile station (MS) time zone change trigger is enabled or not.	All levels
	If this trigger is enabled, an MS time zone change usually results in the CDR being updated with the charging information and then closed.	none

Sample Output

```

show unified-edge ggsn-pgw charging trigger-profile
user@host> show unified-edge ggsn-pgw charging trigger-profile
Gateway Name: PGW
Profile Name: p_tp
Profile ID : 1
Profile Name: p_tp
Profile ID : 1
Time Limit: None
Volume Limit: 1024 Byte (Uplink and Downlink Combined)
PLMN change trigger: Enabled
QoS change trigger : Enabled
RAT change trigger : Enabled
SGSN/SGW change trigger : Enabled
User location change trigger: Enabled
MS Timezone change trigger: Enabled

```

show unified-edge sgw charging local-persistent-storage statistics

Syntax	show unified-edge sgw charging local-persistent-storage statistics <gateway gateway>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Display the storage statistics of the Charging Data Record (CDR) files on the local Routing Engine disk for the Serving Gateways (S-GWs). If a gateway name is not specified, then the status for all S-GWs is displayed.
Options	none —Display the storage statistics for all S-GWs. gateway gateway —(Optional) Display the storage statistics for the specified gateway.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear unified-edge sgw charging local-persistent-storage statistics on page 1116
List of Sample Output	show unified-edge sgw charging local-persistent-storage statistics on page 1152
Output Fields	Table 84 on page 1148 lists the output fields for the show unified-edge sgw charging local-persistent-storage statistics command. Output fields are listed in the approximate order in which they appear.

Table 84: show unified-edge sgw charging local-persistent-storage statistics Output Fields

Field Name	Field Description
Batch Messages received	Total number of batch messages sent from services PICs to the Routing Engine disk. CDRs generated in services PICs are sent to the local Routing Engine disk as batch messages.
Batch Responses sent	Total number of responses sent to the batch messages received.
Invalid Messages received	Total number of invalid batch messages sent from services PICs to the Routing Engine disk.
Number of temp log files opened	<p>Total number of temporary CDR files opened on the Routing Engine disk.</p> <p>These files are closed and copied from the temporary location to a final location (/opt/mobility/charging/ggsn/final_log) within the same Routing Engine disk from where the files can be transferred using SSH FTP (SFTP). Files are closed when the file size, file age, or the maximum number of CDRs added to the file reaches the configured limit (or the default limit, if the limit is not configured).</p>

Table 84: show unified-edge sgw charging local-persistent-storage statistics Output Fields (*continued*)

Field Name	Field Description
Number of journal files opened	Total number of open journal files. Journal files are used to remove any unfinished file writes from the temporary log files if a daemon or router crash interrupts the kernel file write. When the daemon or router come back up, the journal log files are read to ensure that the contents of the temporary log file are sane. If there is any unfinished CDR data, the temporary log file is truncated to the last-known successful file write. For each temporary log CDR file, a separate journal file is opened.
Number of journal files closed	Total number of journal files closed.
Number of CDR log files closed	Total number of temporary CDR log files closed. Authorized users can use SFTP to transfer these files from the <code>/opt/mobility/charging/ggsn/final_log</code> location.
Number of CDR files closed due to file-age	Total number of temporary CDR log files closed because the age of the files reached the configured limit (or the default limit, if the limit is not configured). The default file age is 120 minutes.
Number of CDR files closed due to file-size	Total number of temporary CDR log files closed because the size of the files reached the configured limit (or the default limit, if the limit is not configured). The default file size is 10 megabytes (MB).
Number of CDR files closed due to cdr-count	Total number of temporary CDR log files closed because the maximum number of CDRs added to the files reached the configured limit. There is no default limit.
Abnormal file closures	Total number of abnormal temporary CDR log file closures. This counter is incremented when the charging daemon comes up after a system reboot or crash and temporary CDR log file closures are triggered.
Normal file closures	Total number of temporary CDR log file closures. This counter is incremented when changes in the configuration, such as a change in the file format, trigger temporary CDR log file closures.
Number of CDR log files closed in TS_32_297 format	Total number of closed temporary CDR log files that are compliant with the format specified in the 32297 technical specification release.
Number of CDR log files closed in raw asn1 format	Total number of closed temporary CDR log files that are in the raw ASN1 format.
Total number of CDRs backed up	Total number of CDRs backed up to the standby Routing Engine.

Table 84: show unified-edge sgw charging local-persistent-storage statistics Output Fields (*continued*)

Field Name	Field Description
Disk Full messages sent	<p>Total number of messages sent by the Routing Engine to the services PICs to indicate that its disk is already full and is unable to accept any more charging data.</p> <p>Use SFTP to transfer the files from the <code>/opt/mobility/charging/ggsn/final_log</code> location to free disk space, or remove the disk and copy the files.</p> <p>You can remove the disk by issuing the following commands in this order:</p> <ul style="list-style-type: none"> • request system storage unified-edge charging media stop • request system storage unified-edge media eject
Disk Full resolve messages sent	Total number of disk full resolve messages sent. When the disk space is freed, the Routing Engine sends messages to the services PICs indicating that it can receive charging data.
Number of async IO reqs written	Number of asynchronous I/O requests written. This counter is incremented once for every write operation into the temporary log CDR file.
Disk space status	<p>Indicates whether disk space is available for storage. The possible values are:</p> <ul style="list-style-type: none"> • DISK_AVAILABLE • DISK_AT_WATERMARK_LEVEL1 • DISK_AT_WATERMARK_LEVEL2 • DISK_AT_WATERMARK_LEVEL3 • DISK_OFFLINE—Indicates that a disk is not present or the request system storage unified-edge charging media stop command has been issued. • DISK_OFFLINE_PENDING—Indicates whether any CDRs are being written or mirrored on the backup Routing Engine. This interim status message is displayed after the request system storage unified-edge charging media stop command has been issued but before the disk goes offline.
Watermark level1 at (MB)	<p>Indicates the percentage of the total Routing Engine disk space configured for storage. By default, watermark level 1 is set to 70 percent of the total disk space.</p> <p>When this limit is reached, an alert (if configured) is sent and you can take corrective measures to free the disk space.</p>
Watermark level2 at (MB)	<p>Indicates the percentage of the total Routing Engine disk space for storage. By default, watermark level 2 is set to 80 percent of the total disk space.</p> <p>When this limit is reached, an alert (if configured) is sent and you can take corrective measures to free the disk space.</p>

Table 84: show unified-edge sgw charging local-persistent-storage statistics Output Fields (*continued*)

Field Name	Field Description
Watermark level3 at (MB)	<p>Indicates the percentage of the total Routing Engine disk space configured for storage. By default, watermark level 3 is set to 90 percent of the total disk space.</p> <p>When this limit is reached, an alert (if configured) is sent and you can take any corrective measures to free the disk space. Otherwise, the services PICs stop sending the charging data to the Routing Engine disk and you must transfer the files via SFTP to free the disk space. However, the charging data is not lost because it is buffered in the services PICs. Services PICs can buffer up to a maximum of 2 GB of data after which a call admission control (CAC) is triggered.</p>
Temporary CDR log file Statistics —The following information for the temporary CDR log files is displayed only if temporary CDR log files are currently open.	
File Name	Name of the temporary CDR log file.
Journal file name	Name of the journal file.
Current number of CDRs	Total number of CDRs currently added to the temporary CDR log file.
Current file size (bytes)	Current size, in bytes, of the temporary CDR log file.
File age trigger (mins)	Configured duration, in minutes, after which the temporary CDR log file is closed, in minutes. If this parameter is not configured, then the default value is displayed.
File size trigger (bytes)	Configured size, in bytes, that the temporary CDR log file can reach after which it is closed. If this parameter is not configured, then the default value is displayed.
CDR count trigger	Configured maximum number of CDRs that can be added to the temporary CDR log file, after which it is closed. If this parameter is not configured, then the default value is displayed.
Global Statistics	
Disk Offline messages sent	<p>Total number of messages sent by the Routing Engine to the services PICs to indicate that its disk is offline or is not mounted, and that it is unable to accept any more charging data.</p> <p>You can configure the disk (storage media) to store charging data by issuing these commands:</p> <ul style="list-style-type: none"> • request system storage unified-edge media prepare • request system storage unified-edge charging media start
Disk Available messages sent	When the disk is prepared and mounted, the Routing Engine sends messages to the services PICs to indicate that it can now receive charging data. This field indicates the total number of these messages sent.

Table 84: show unified-edge sgw charging local-persistent-storage statistics Output Fields (*continued*)

Field Name	Field Description
Number of CDR storage files on disk	Total number of CDR files stored on the local Routing Engine disk.
Current storage space in use (MB)	Storage space, in MB, that is currently being used.
Available storage space on disk (MB)	Total free space, in MB, available for storage on the disk.
Total storage space on disk (MB)	Total storage space, in MB, on the disk.

Sample Output

```

show unified-edge sgw charging local-persistent-storage statistics
user@host> show unified-edge sgw charging local-persistent-storage statistics
Gateway: SGW
Charging local-persistent-storage Statistics
  Batch Messages received           : 76
  Batch Responses sent              : 76
  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    : 2095
  Disk Full messages sent           : 0
  Disk Full resolve messages sent   : 0
  Number of async IO reqs written   : 76
  Disk space status                 : DISK_AVAILABLE
  Watermark level1 at(MB)           : 618(70%)
  Watermark level2 at(MB)           : 707(80%)
  Watermark level3 at(MB)           : 795(90%)

Temporary CDR log file Statistics
File Name: /opt/mobility/charging/ggsn/temp_log/templog_file_1.log
  Journal file name                  : /opt/mobility/charging/ggsn/jrnl/jrnl_1.log
  Current number of CDRs             : 2095
  Current file size(bytes)           : 553028
  File age trigger(mins)             : 60
  File size trigger(bytes)           : 10485760
  CDR count trigger                  : 0

Global Statistics
  Disk Offline messages sent         : 0
  Disk Available messages sent       : 0
  Number of CDR storage files on disk : 0
  Current storage space in use(MB)    : 301
  Available storage space on disk(MB) : 583

```

Total storage space on disk(MB) : 884

show unified-edge sgw charging path statistics

Syntax	show unified-edge sgw charging path statistics <brief detail> <fpc-slot <i>slot-number</i>> <gateway-name <i>name</i>> <gtp-peer-addr <i>ipv4-address</i>> <gtp-peer-name <i>peer-name</i>> <pic-slot <i>slot-number</i>>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Display the path management message statistics (between the charging data function [CDF] and the charging gateway function [CGF] servers) on one or more Serving Gateways (S-GWs). If a gateway name is not specified, then the path management statistics for all S-GWs are displayed.
Options	<p>none—(Same as brief) Display the path management message statistics for all S-GWs.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>The brief option displays the statistics per S-GW for all services PICs. The detail option displays the statistics per S-GW for each services PIC.</p> <p>fpc-slot <i>slot-number</i>—(Optional) Display the path management message statistics for the specified FPC slot number.</p> <p>gateway-name <i>name</i>—(Optional) Display the path management message statistics for the specified gateway.</p> <p>gtp-peer-addr <i>ipv4-address</i>—(Optional) Display the path management message statistics for the GTP Prime peer with the specified IPv4 address.</p> <p>gtp-peer-name <i>peer-name</i>—(Optional) Display the path management message statistics for the GTP Prime peer with the specified name.</p> <p>pic-slot <i>slot-number</i>—(Optional) Display the path management message statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• clear unified-edge sgw charging path statistics on page 1117• show unified-edge sgw charging path status on page 1159
List of Sample Output	show unified-edge sgw charging path statistics brief on page 1156 show unified-edge sgw charging path statistics detail on page 1157

Output Fields Table 85 on page 1155 lists the output fields for the **show unified-edge sgw charging path statistics** command. Output fields are listed in the approximate order in which they appear.

Table 85: show unified-edge sgw charging path statistics Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the S-GW.	All levels
Charging Path Statistics		
FPC/PIC	FPC slot number and PIC slot number for which the statistics are displayed.	detail
CGF Address	Address of the CGF server (GTP Prime peer).	All levels
CGF Server Name	Name of the CGF server (GTP Prime peer).	All levels
Echo Requests Rx	Total number of echo requests received by the CDF from the CGF server.	All levels
Echo Responses Tx	Total number of echo responses transmitted by the CDF to the CGF server.	All levels
Echo Responses Rx	Total number of echo responses received by the CDF from the CGF server.	All levels
Echo Requests Tx	Total number of echo requests transmitted by the CDF to the CGF server.	All levels
Node-Alive Requests Rx	Total number of node alive requests received by the CDF from the CGF server.	All levels
Node-Alive Responses Tx	Total number of responses transmitted by the CDF to the node alive requests received from the CGF server.	All levels
Version Not Supported Rx	Total number of Version Not Supported messages received by the CDF from the CGF server. The CGF server sends these messages to the CDF to indicate that the GTP Prime messages sent by the CDF are incompatible with the GTP Prime version supported by the CGF server.	All levels
Version Not Supported Tx	Total number of Version Not Supported messages transmitted by the CDF to the CGF server. The CDF sends these messages to indicate that the GTP Prime messages sent by the CGF server are incompatible with the GTP Prime version supported by the CDF.	All levels
Echo Requests timed out	Total number of echo requests sent by the CDF for which there were no responses from the CGF server and that have timed out.	All levels
Echo Interval	Configured echo interval, in seconds. If the echo interval is not configured, then the default value is displayed.	All levels
Down Detection Interval	Configured down detect time, in seconds. If the down detect time is not configured, then the default value is displayed.	All levels
Reconnect Time Interval	Configured reconnect time, in seconds. If the reconnect time is not configured, then the default value is displayed.	All levels

Table 85: show unified-edge sgw charging path statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
Destination Port	Configured destination port. If the destination port is not configured, then the default port (3386) is displayed.	All levels
Pending Queue Size	Configured pending queue size. If the pending queue size is not configured, then the default value (1024) is displayed.	All levels
Path Manager FPC Slot	FPC slot that manages the path management messages.	All levels
Path Manager PIC Slot	PIC slot that manages the path management messages.	All levels
Path Manager Port	Port used for path management messages.	All levels
T3 Response Time Interval	Configured T3 response time interval, in seconds. If the T3 response time interval is not configured, then the default value (5 seconds) is displayed.	All levels
Source Interface Valid	Indicates whether the source interface is valid or not.	All levels
GTPP Header Type	Configured header type for the GTP Prime messages.	All levels
N3 Requests	Configured value for N3 requests . If the N3 requests is not configured, then the default value (3) is displayed.	All levels
Local Address	Address of the local loopback source interface from which the GTP Prime packets are sent to the CGF server.	All levels
GTPP Version	Configured version that is supported on the configured local loopback source interface's IP address, from which the GTP Prime packets are sent to the CGF server.	All levels
Transport Protocol	Configured transport protocol for sending the GTP Prime packets from CDF to the CGF server.	All levels
TCP Port Range Start	Start of the range of source ports from which the TCP connection from each services PIC to the CGF server can originate. The S-GW assigns a range of source ports internally.	All levels
TCP Port Range End	End of the range of source ports from which the TCP connection from each services PIC to the CGF server can originate. The S-GW assigns a range of source ports internally.	All levels
TCP Connection State	Indicates whether the TCP connection state on the services PIC has been established or not.	detail

Sample Output

```

show unified-edge sgw charging path statistics brief
user@host> show unified-edge sgw charging path statistics brief
Gateway: SGW
Charging Path Statistics

```

```

CGF Address           : 2.2.2.2          CGF Server Name       : s_cgf
Echo Requests         Rx: 0              Echo Responses        Tx: 0
Echo Responses        Rx: 0              Echo Requests         Tx: 0
Node-Alive Requests   Rx: 0              Node-Alive Responses  Tx: 0
Version Not Supported Rx: 0              Version Not Supported Tx: 0
Echo Requests timed out : 0              Echo Interval         : 0
Down Detection Interval : 10              Reconnect Time Interval : 60
Destination Port      : 3386              Pending Queue Size     : 1000
Path Manager FPC Slot : 2                 Path Manager PIC Slot  : 0
T3 Response Time Interval : 5              Path Manager Port      : 30275
Source Interface Valid : Yes               GTPP Header Type       : long
N3 Requests           : 1                 Local Address          : 13.4.1.1

GTPP Version          : V0                 Transport Protocol     : TCP
TCP Port Range Start  : 30277              TCP Port Range End     : 30308

```

Gateway: SGW2
Charging Path Statistics

```

CGF Address           : 2.2.2.2          CGF Server Name       : s_cgf
Echo Requests         Rx: 0              Echo Responses        Tx: 0
Echo Responses        Rx: 0              Echo Requests         Tx: 0
Node-Alive Requests   Rx: 0              Node-Alive Responses  Tx: 0
Version Not Supported Rx: 0              Version Not Supported Tx: 0
Echo Requests timed out : 0              Echo Interval         : 0
Down Detection Interval : 10              Reconnect Time Interval : 60
Destination Port      : 3386              Pending Queue Size     : 1000
Path Manager FPC Slot : 2                 Path Manager PIC Slot  : 1
T3 Response Time Interval : 5              Path Manager Port      : 30241
Source Interface Valid : Yes               GTPP Header Type       : long
N3 Requests           : 1                 Local Address          : 12.4.1.1

GTPP Version          : V0                 Transport Protocol     : TCP
TCP Port Range Start  : 30243              TCP Port Range End     : 30274

```

**show unified-edge sgw
charging path
statistics detail**

user@host> show unified-edge sgw charging path statistics detail

Gateway: SGW
Charging Path Statistics
FPC/PIC: 2/0

```

CGF Address           : 2.2.2.2          CGF Server Name       : s_cgf
Echo Requests         Rx: 0              Echo Responses        Tx: 0
Echo Responses        Rx: 0              Echo Requests         Tx: 0
Node-Alive Requests   Rx: 0              Node-Alive Responses  Tx: 0
Version Not Supported Rx: 0              Version Not Supported Tx: 0
Echo Requests timed out : 0              Echo Interval         : 0
Down Detection Interval : 10              Reconnect Time Interval : 60
Destination Port      : 3386              Pending Queue Size     : 1000
Path Manager FPC Slot : 2                 Path Manager PIC Slot  : 0
T3 Response Time Interval : 5              Path Manager Port      : 30275
Source Interface Valid : Yes               GTPP Header Type       : long
N3 Requests           : 1                 Local Address          : 13.4.1.1

GTPP Version          : V0                 Transport Protocol     : TCP
TCP Port Range Start  : 30277              TCP Port Range End     : 30308
TCP Connection State   : Established
FPC/PIC: 5/0

```

```

CGF Address           : 2.2.2.2          CGF Server Name       : s_cgf
Echo Requests         Rx: 0              Echo Responses        Tx: 0

```

Echo Responses	Rx: 0	Echo Requests	Tx: 0
Node-Alive Requests	Rx: 0	Node-Alive Responses	Tx: 0
Version Not Supported	Rx: 0	Version Not Supported	Tx: 0
Echo Requests timed out	: 0	Echo Interval	: 0
Down Detection Interval	: 10	Reconnect Time Interval	: 60
Destination Port	: 3386	Pending Queue Size	: 1000
Path Manager FPC Slot	: 2	Path Manager PIC Slot	: 0
T3 Response Time Interval	: 5	Path Manager Port	: 30275
Source Interface Valid	: Yes	GTPP Header Type	: long
N3 Requests	: 1	Local Address	: 13.4.1.1
GTPP Version	: V0	Transport Protocol	: TCP
TCP Port Range Start	: 30277	TCP Port Range End	: 30308
TCP Connection State	: Not Established		

Gateway: SGW2

Charging Path Statistics

FPC/PIC: 2/1

CGF Address	: 2.2.2.2	CGF Server Name	: s_cgf
Echo Requests	Rx: 0	Echo Responses	Tx: 0
Echo Responses	Rx: 0	Echo Requests	Tx: 0
Node-Alive Requests	Rx: 0	Node-Alive Responses	Tx: 0
Version Not Supported	Rx: 0	Version Not Supported	Tx: 0
Echo Requests timed out	: 0	Echo Interval	: 0
Down Detection Interval	: 10	Reconnect Time Interval	: 60
Destination Port	: 3386	Pending Queue Size	: 1000
Path Manager FPC Slot	: 2	Path Manager PIC Slot	: 1
T3 Response Time Interval	: 5	Path Manager Port	: 30241
Source Interface Valid	: Yes	GTPP Header Type	: long
N3 Requests	: 1	Local Address	: 12.4.1.1
GTPP Version	: V0	Transport Protocol	: TCP
TCP Port Range Start	: 30243	TCP Port Range End	: 30274
TCP Connection State	: Not Established		

FPC/PIC: 5/1

CGF Address	: 2.2.2.2	CGF Server Name	: s_cgf
Echo Requests	Rx: 0	Echo Responses	Tx: 0
Echo Responses	Rx: 0	Echo Requests	Tx: 0
Node-Alive Requests	Rx: 0	Node-Alive Responses	Tx: 0
Version Not Supported	Rx: 0	Version Not Supported	Tx: 0
Echo Requests timed out	: 0	Echo Interval	: 0
Down Detection Interval	: 10	Reconnect Time Interval	: 60
Destination Port	: 3386	Pending Queue Size	: 1000
Path Manager FPC Slot	: 2	Path Manager PIC Slot	: 1
T3 Response Time Interval	: 5	Path Manager Port	: 30241
Source Interface Valid	: Yes	GTPP Header Type	: long
N3 Requests	: 1	Local Address	: 12.4.1.1
GTPP Version	: V0	Transport Protocol	: TCP
TCP Port Range Start	: 30243	TCP Port Range End	: 30274
TCP Connection State	: Not Established		

show unified-edge sgw charging path status

Syntax `show unified-edge sgw charging path status`
`<brief | detail>`
`<fpc-slot slot-number>`
`<gateway-name name>`
`<gtp-peer-addr ipv4-address>`
`<gtp-peer-name peer-name>`
`<pic-slot slot-number>`

Release Information Command introduced in Junos OS Mobility Release 11.4W.

Description Display the status of the configured GPRS tunneling protocol (GTP) Prime peers for the Serving Gateways (S-GWs). If a gateway name is not specified, then the status for all S-GWs is displayed.

The status includes information about whether the GTP Prime peers are connected, down, or still in the process of establishing a connection, and whether the echo messages are enabled or disabled



NOTE: In charging, the terms GTP Prime peers and charging gateway function (CGF) server are used interchangeably.

Options `none`—(Same as `brief`) Display the status of the configured GTP Prime peers for all S-GWs.

`brief | detail`—(Optional) Display the specified level of output.

`fpc-slot slot-number`—(Optional) Display the status of the configured GTP Prime peers for the specified FPC slot number.

`gtp-peer-addr ipv4-address`—(Optional) Display the status of the GTP Prime peer with the specified IPv4 address.

`gtp-peer-name peer-name`—(Optional) Display the status of the GTP Prime peer with the specified name.

`pic-slot slot-number`—(Optional) Display the status of the configured GTP Prime peers for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

Required Privilege Level `view`

Related Documentation • [show unified-edge sgw charging path statistics on page 1154](#)

List of Sample Output [show unified-edge sgw charging path status brief on page 1160](#)
[show unified-edge sgw charging path status detail on page 1160](#)

Output Fields Table 86 on page 1160 lists the output fields for the **show unified-edge sgw charging path status** command. Output fields are listed in the approximate order in which they appear.

Table 86: show unified-edge sgw charging path status Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the S-GW.	All levels
Peer-Address	Address of the charging gateway function (CGF) server (GTP Prime peer).	All levels
Peer-Name	Name of the CGF server (GTP Prime peer).	All levels
Local-Address	IPv4 address of the local loopback source interface from where the GTP Prime packets are sent to the CGF server (GTP Prime peer).	All levels
Status	Status of the CGF server: <ul style="list-style-type: none"> • Connected • Down • In-Progress 	All levels
Echo	Indicates whether echo messages are enabled or disabled. The possible values are: <ul style="list-style-type: none"> • Enabled or Disabled for UDP connections • N/A (Not Applicable) for TCP connections 	All levels
Cause	Probable cause for the current status of the CGF peer. This field is displayed only when the CGF server is down or the connection has not been established.	detail
FPC/PIC	FPC and PIC slot numbers.	detail

Sample Output

```

show unified-edge sgw charging path status brief
user@host> show unified-edge sgw charging path status brief
Gateway: SGW
Charging Path Status
Peer-Address  Peer-Name  Local-Address  Status      Echo
3.3.3.3       test       13.4.1.1       In-Progress N/A
2.2.2.2       s_cgf      13.4.1.1       Connected   N/A

```

```

show unified-edge sgw charging path status detail
user@host> show unified-edge sgw charging path status detail
Gateway: SGW
Charging Path Status

FPC/PIC 2/1
Peer-Address 3.3.3.3
Peer-Name test
Local-Address 13.4.1.1
Status Down
Cause Server Not Responding

```

Echo	N/A
Peer-Address	2.2.2.2
Peer-Name	s_cgf
Local-Address	13.4.1.1
Status	Connected
Echo	N/A

show unified-edge sgw charging service-mode

Syntax	show unified-edge sgw charging service-mode gateway-name <i>gateway-name</i> <brief detail> <charging-profile-name <i>profile-name</i>> <transport-profile-name <i>profile-name</i>>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Display the charging service mode information for the specified Serving Gateway (S-GW).
Options	<p>gateway-name <i>gateway-name</i>—Display the charging service mode information for the specified gateway.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>charging-profile-name <i>profile-name</i>—(Optional) Display the service mode information for the specified charging profile.</p> <p>transport-profile-name <i>profile-name</i>—(Optional) Display the service mode information for the specified transport profile.</p>
Required Privilege Level	view
List of Sample Output	show unified-edge sgw charging service-mode gateway SGW brief on page 1163 show unified-edge sgw charging service-mode gateway SGW detail on page 1163
Output Fields	Table 87 on page 1162 lists the output fields for the show unified-edge sgw charging service-mode command. Output fields are listed in the approximate order in which they appear.

Table 87: show unified-edge sgw charging service-mode Output Fields

Field Name	Field Description	Level of Output
Gateway Name	Name of the S-GW.	All levels
Service Mode	Service mode for the gateway. The following service modes are possible: <ul style="list-style-type: none"> Operational—Gateway is in operational mode. Maintenance—Gateway is in maintenance mode. MM Active Phase—In this mode, you can make changes to any of the configuration options under the [edit unified-edge gateways sgw gateway-name charging charging-profiles] or the [edit unified-edge gateways sgw gateway-name charging transport-profiles] hierarchy levels. MM In/Out Phase—In this mode, you cannot make changes to the configuration options under the [edit unified-edge gateways sgw gateway-name charging charging-profiles] or the [edit unified-edge gateways sgw gateway-name charging transport-profiles] hierarchy levels. 	All levels
Charging Profile(s) or Charging Profile	Name of the charging profile.	All levels

Table 87: show unified-edge sgw charging service-mode Output Fields (*continued*)

Field Name	Field Description	Level of Output
Service Mode	Service mode for the charging profile.	All levels
Transport Profile(s) or Transport Profile	Name of the transport profile.	brief
Service Mode	Service mode for the transport profile.	All levels
Pending Maintenance Mode Ready Ack	Lists the components or modules that are not yet ready to accept the configuration changes. Maintenance mode becomes active only after all the components or modules are ready to accept these changes.	detail

Sample Output

```

show unified-edge sgw charging service-mode gateway SGW brief
user@host> show unified-edge sgw charging service-mode gateway SGW brief
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       : SGW
Service Mode       : Operational

Charging Profile(s)      Service Mode
p_juniper              Operational
Transport Profile(s)     Service Mode
p_tsp                  Operational

show unified-edge sgw charging service-mode gateway SGW detail
user@host> show unified-edge sgw charging service-mode gateway SGW detail
Gateway Name       : SGW
Service Mode       : Operational

Charging Profile: p_juniper
Service Mode      : Operational
Transport Profile: p_tsp
Service Mode      : Operational

```

show unified-edge sgw charging transfer statistics

Syntax	<pre>show unified-edge sgw charging transfer statistics <brief detail> <fpc-slot slot-number> <gateway-name name> <pic-slot slot-number> <transport-profile-name profile-name></pre>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Display the transfer statistics for the configured transport profiles on one or more Serving Gateways (S-GWs). If a gateway name is not specified, then the transfer statistics for all S-GWs are displayed.
Options	<p>none—(Same as brief) Display the transfer statistics for all S-GWs.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>fpc-slot slot-number—(Optional) Display the transfer statistics for the specified FPC slot number.</p> <p>gateway-name name—(Optional) Display the transfer statistics for the specified gateway.</p> <p>pic-slot slot-number—(Optional) Display the transfer statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.</p> <p>transport-profile-name profile-name—(Optional) Display the transfer statistics for the specified transport profile.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear unified-edge sgw charging transfer statistics on page 1118
List of Sample Output	show unified-edge sgw charging transfer statistics brief on page 1166 show unified-edge sgw charging transfer statistics detail on page 1166
Output Fields	Table 88 on page 1164 lists the output fields for the show unified-edge sgw charging transfer statistics command. Output fields are listed in the approximate order in which they appear.

Table 88: show unified-edge sgw charging transfer statistics Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the S-GW.	All levels
Transport-Profile	Name of the transport profile.	All levels

Table 88: show unified-edge sgw charging transfer statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
Redirection Requests Rx	<p>Total number of redirection request messages received by the charging data function (CDF) from the charging gateway function (CGF) server.</p> <p>The CGF server sends these messages to inform the CDF about the following:</p> <ul style="list-style-type: none"> • The CGF server is about to stop service (possibly due to an error or for maintenance). • The next node in the chain (such as a billing server) has lost its connection to the CGF server. 	All levels
Redirection Responses Tx	Total number of redirection response messages transmitted as responses to the redirection requests received. Redirection response messages indicate whether a redirection request message was successful or not.	All levels
DRT Responses Rx	Total number of Data Record Transfer (DRT) response messages received for the DRT request messages sent. DRT response messages indicate whether a DRT request was successful or not.	All levels
DRT Requests Tx	Total number of DRT request messages transmitted to the CGF server. These messages are used to transfer Charging Data Records (CDRs) from the CDF to the CGF server.	All levels
DRT successful Responses Rx	Total number of successful DRT response messages received for the DRT request messages sent.	All levels
DRT Error Responses Rx	Total number of DRT error response messages received for the DRT request messages sent.	All levels
DRT Requests timed out	Total number of DRT requests sent that timed out before receiving a response from the CGF server.	All levels
CGF Switch Back Times	Total number of times the CGF servers were switched, which indicates the number of times that the CGF servers were either offline or down for maintenance.	All levels
Batch Requests Tx	Total number of batch requests transmitted from services PICs for a transport profile.	All levels
Batch Response Errors Rx	Total number of error responses, sent by the Routing Engine to the services PICs, for the batch requests messages received.	All levels
Batch CDR's Tx	Total number of CDRs transmitted from services PICs to the Routing Engine.	All levels
CDR Count	Total number of CDRs transmitted to the CGF server.	All levels
Total WFA	Total number of request messages awaiting acknowledgements from the Routing Engine or the CGF server.	All levels
FPC/PIC	FPC and PIC slot numbers.	detail

Sample Output

```

show unified-edge sgw charging transfer statistics brief
user@host> show unified-edge sgw charging transfer statistics brief
Gateway: SGW
Charging Transfer Statistics
Transport-Profile : s_tsp
  Redirection Requests Rx: 0      Redirection Responses Tx: 0
  DRT Responses Rx: 102    DRT Requests Tx: 102
  DRT successful Responses Rx: 102 DRT Error Responses Rx: 0
  DRT Requests timed out : 0    CGF Switch Back Times : 0
  Batch Requests Tx: 0      Batch Response Errors Rx: 0
  Batch CDR's Tx: 0        CDR Count : 102
  Total WFA : 0

Transport-Profile : s_tsp2
  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: 0      Batch Response Errors Rx: 0
  Batch CDR's Tx: 0        CDR Count : 0
  Total WFA : 0

show unified-edge sgw charging transfer statistics detail
user@host> show unified-edge sgw charging transfer statistics detail
Gateway: SGW
Charging Transfer Statistics
FPC/PIC: 2/1
Transport-profile : s_tsp
  Redirection Requests Rx: 0      Redirection Responses Tx: 0
  DRT Responses Rx: 65    DRT Requests Tx: 65
  DRT successful Responses Rx: 65 DRT Error Responses Rx: 0
  DRT Requests timed out : 0    CGF Switch Back Times : 0
  Batch Requests Tx: 0      Batch Response Errors Rx: 0
  Batch CDR's Tx: 0        CDR Count : 65
  Total WFA : 0

Transport-profile : s_tsp2
  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: 0      Batch Response Errors Rx: 0
  Batch CDR's Tx: 0        CDR Count : 0
  Total WFA : 0

FPC/PIC: 3/1
Transport-profile : s_tsp
  Redirection Requests Rx: 0      Redirection Responses Tx: 0
  DRT Responses Rx: 51    DRT Requests Tx: 51
  DRT successful Responses Rx: 51 DRT Error Responses Rx: 0
  DRT Requests timed out : 0    CGF Switch Back Times : 0
  Batch Requests Tx: 0      Batch Response Errors Rx: 0
  Batch CDR's Tx: 0        CDR Count : 51
  Total WFA : 0

Transport-profile : s_tsp2
  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: 0	Batch Response Errors	Rx: 0
Batch CDR's	Tx: 0	CDR Count	: 0
Total WFA	: 0		

show unified-edge sgw charging transfer status

Syntax	show unified-edge sgw charging transfer status <brief detail> <fpc-slot <i>slot-number</i>> <gateway-name <i>name</i>> <pic-slot <i>slot-number</i>> <transport-profile-name <i>profile-name</i>>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Display the Charging Data Record (CDR) transfer status for the transport profiles on one or more Serving Gateways (S-GWs). If a gateway name is not specified, then the transfer status for all S-GWs are displayed.
Options	<p>none—(Same as brief) Display the total number of unacknowledged and buffered CDRs for the configured transport profiles for all S-GWs.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>fpc-slot <i>slot-number</i>—(Optional) Display the total number of unacknowledged and buffered CDRs for the configured transport profiles for the specified FPC slot number.</p> <p>gateway-name <i>name</i>—(Optional) Display the total number of unacknowledged and buffered CDRs for the configured transport profiles for the specified gateway.</p> <p>pic-slot <i>slot-number</i>—(Optional) Display the total number of unacknowledged and buffered CDRs for the configured transport profiles for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.</p> <p>transport-profile-name <i>profile-name</i>—(Optional) Display the total number of unacknowledged and buffered CDRs for the configured transport profiles for the specified transport profile.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show unified-edge sgw charging transfer statistics on page 1164
List of Sample Output	show unified-edge sgw charging transfer status brief on page 1169 show unified-edge sgw charging transfer status detail on page 1169
Output Fields	Table 89 on page 1168 lists the output fields for the show unified-edge sgw charging transfer status command. Output fields are listed in the approximate order in which they appear.

Table 89: show unified-edge sgw charging transfer status Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the S-GW.	All levels

Table 89: show unified-edge sgw charging transfer status Output Fields (*continued*)

FPC/PIC	FPC and PIC slot numbers.	detail
Transport-Profile	Name of the transport profile.	All levels
Transport-profile Id	ID of the transport profile.	detail
Total UnAck CDR's	Total number of CDRs (for the transport profile) sent to the charging gateway function (CGF) servers for which no acknowledgements were received.	All levels
Total Buffered CDR's	Total number of buffered CDRs (for the transport profile) in the services PICs.	All levels

Sample Output

```

show unified-edge sgw charging transfer status brief
user@host> show unified-edge sgw charging transfer status brief
Gateway: SGW
Charging Transfer Status
Transport-Profile : s_tsp
  Total UnAck CDR's      : 0
  Total Buffered CDR's   : 10

Transport-Profile : s_tsp2
  Total UnAck CDR's      : 0
  Total Buffered CDR's   : 0

```

```

show unified-edge sgw charging transfer status detail
user@host> show unified-edge sgw charging transfer status detail
Gateway: SGW
Charging Transfer Status
FPC/PIC: 2/1
Transport-profile      : s_tsp
Transport-profile Id   : 1
Total UnAck CDR's     : 0
Total Buffered CDR's   : 2

Transport-profile      : s_tsp2
Transport-profile Id   : 2
Total UnAck CDR's     : 0
Total Buffered CDR's   : 0

FPC/PIC: 3/1
Transport-profile      : s_tsp
Transport-profile Id   : 1
Total UnAck CDR's     : 0
Total Buffered CDR's   : 8

Transport-profile      : s_tsp2
Transport-profile Id   : 2
Total UnAck CDR's     : 0
Total Buffered CDR's   : 0

```

show unified-edge sgw charging trigger-profile

Syntax	show unified-edge ggsn-pgw charging trigger-profile <gateway <i>gateway-name</i>> <trigger-profile-name <i>profile-name</i>>
Release Information	Statement introduced in Junos OS Mobility Release 11.4W.
Description	Display the configuration of the trigger profiles for one or more Serving Gateways (S-GWs). If a gateway name is not specified, then information for all S-GWs are displayed.
Options	gateway <i>gateway-name</i> —(Optional) Display the trigger profile information for the specified gateway. trigger-profile-name <i>profile-name</i> —(Optional) Display the information for the specified trigger profile.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • trigger-profiles on page 846
List of Sample Output	show unified-edge sgw charging trigger-profile gateway SGW on page 1171
Output Fields	Table 90 on page 1170 lists the output fields for the show unified-edge sgw charging trigger-profile command. Output fields are listed in the approximate order in which they appear.

Table 90: show unified-edge sgw charging trigger-profile Output Fields

Field Name	Field Description
Gateway Name	Name of the S-GW
Profile Name	Name of the trigger profile.
Profile ID	ID of the trigger profile.
Time Limit	The time limit for the trigger profile, if any.
Volume Limit	The volume limit (in bytes) for the trigger profile, if any.
PLMN change trigger	<p>Indicates whether the public land mobile network (PLMN) change trigger is enabled or not.</p> <p>If this trigger is enabled, a PLMN change usually results in the Charging Data Record (CDR) being updated with the charging information and then closed.</p>
QoS change trigger	<p>Indicates whether the QoS change trigger is enabled or not.</p> <p>If this trigger is enabled, a QoS change usually results in a container being added to the CDR.</p>

Table 90: show unified-edge sgw charging trigger-profile Output Fields (*continued*)

Field Name	Field Description
RAT change trigger	Indicates whether the RAT change trigger is enabled or not. If this trigger is enabled, a RAT change usually results in the CDR being updated with the charging information and then closed.
SGSN/MME change trigger	Indicates whether the Serving GPRS Support Node (SGSN) or Mobility Management Entity (MME) change trigger is enabled or not. If this trigger is enabled, then for each change, the SGSN or MME address is recorded in the CDR.
User location change trigger	Indicates whether the user-location change trigger is enabled or not. If this trigger is enabled, a user location change usually results in the current container being closed and added to the CDR.
MS Timezone change trigger	Indicates whether the Mobile Station (MS) time zone change trigger is enabled. If this trigger is enabled, an MS time zone change usually results in the CDR being updated with the charging information and then closed.

Sample Output

```

show unified-edge sgw charging trigger-profile gateway SGW
user@host> show unified-edge sgw charging trigger-profile gateway SGW
Gateway Name: SGW
Profile Name: s_tp
Profile ID : 1
Profile Name: s_tp
Profile ID : 1
Time Limit: None
Volume Limit: 1024 Byte (Uplink and Downlink Combined)
PLMN change trigger: Enabled
QOS change trigger : Enabled
RAT change trigger : Enabled
SGSN/MME change trigger : Enabled
User location change trigger: Enabled
MS Timezone change trigger: Enabled

```


CHAPTER 33

Class of Service (CoS) Operational Commands

show unified-edge ggsn-pgw qos statistics

Syntax `show unified-edge ggsn-pgw qos statistics`
`<apn apn>`
`<arp arp>`
`<gateway gateway>`
`<gtpv1-arp gtpv1-arp>`
`<qci qci>`
`<traffic-class (background | conversational | interactive | streaming)>`
`<traffic-handling-priority traffic-handling-priority>`

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Display the quality-of-service (QoS) statistics for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then statistics for all GGSNs and P-GWs are displayed.

Options **none**—Display the QoS statistics for all GGSNs and P-GWs.

apn *apn*—(Optional) Display the QoS statistics for the specified access point name (APN).

arp *arp*—(Optional) Display the QoS statistics for the specified GTP version 2 (GTPv2) allocation and retention priority (ARP) value. You can specify an ARP of 1 through 15.

gateway *gateway*—(Optional) Display the QoS statistics for the specified gateway.

gtpv1-arp *gtpv1-arp*—(Optional) Display the QoS statistics for the specified GTPv1 ARP. You can specify a GTPv1 ARP value of 1 through 3.

qci *qci*—(Optional) Display the QoS statistics for the specified QoS Class Identifier (QCI).

traffic-class (*background* | *conversational* | *interactive* | *streaming*)—(Optional) Display the QoS statistics for the specified traffic class.

traffic-handling-priority *traffic-handling-priority*—(Optional) Display the QoS statistics for the specified traffic handling priority. You can specify a priority of 1 through 3.

Required Privilege Level view

List of Sample Output [show unified-edge ggsn-pgw qos statistics on page 1176](#)

Output Fields [Table 91 on page 1174](#) lists the output fields for the `show unified-edge ggsn-pgw qos statistics` command. Output fields are listed in the approximate order in which they appear.

Table 91: show unified-edge ggsn-pgw qos statistics Output Fields

Field Name	Field Description
Gateway	Name of the GGSN or P-GW.
Control plane statistics	

Table 91: show unified-edge ggsn-pgw qos statistics Output Fields (*continued*)

Field Name	Field Description
Session establishment attempts	Number of attempted session establishments.
Successful session establishments	Number of successful session establishments.
MS/peer initiated session deactivations	Number of attempted deactivations initiated by the mobile station (MS) or the GTP peer.
Successful MS/peer initiated deactivations	Number of deactivations initiated by the MS or GTP peer that were successful.
Gateway initiated session deactivations	Number of attempted deactivations initiated by the broadband gateway.
Successful gateway initiated deactivations	Number of deactivations initiated by the broadband gateway that were successful.
Data plane global statistics	
Source address violation packets	Number of incoming GTP packets with an incorrect source address.
Source address violation bytes	Number of octets of incoming GTP packets with an incorrect source address.
Total packets rcvd with non-existent TEIDs	Number of packets received with a nonexistent tunnel endpoint identifier (TEID).
Data plane GTP statistics (Gn/S5/S8)	
Input packets	Number of incoming GTP data packets on the Gn, Gp, S5, and S8 interfaces.
Input bytes	Number of octets of incoming GTP data packets on the Gn, Gp, S5, and S8 interfaces.
Output packets	Number of outgoing GTP data packets on the Gn, Gp, S5, and S8 interfaces.
Output bytes	Number of octets of outgoing GTP data packets on the Gn, Gp, S5, and S8 interfaces.
Discarded packets	Number of discarded GTP data packets on the Gn, Gp, S5, and S8 interfaces.

Table 91: show unified-edge ggsn-pgw qos statistics Output Fields (*continued*)

Field Name	Field Description
Data plane GTP statistics (Gi)	
Input packets	Number of incoming GTP data packets on the Gi interface.
Input bytes	Number of octets of incoming GTP data packets on the Gi interface.
Output packets	Number of outgoing GTP data packets on the Gi interface.
Output bytes	Number of octets of outgoing GTP data packets on the Gi interface.
Discarded packets	Number of discarded GTP data packets on the Gi interface.


Sample Output

```

show unified-edge user@host> show unified-edge ggsn-pgw qos statistics
ggsn-pgw qos      Gateway: PGW1
statistics        Control plane statistics:
                  Session establishment attempts:      1000
                  Successful session establishments:     1000
                  MS/peer initiated session deactivations: 0
                  Successful MS/peer initiated deactivations: 0
                  Gateway initiated session deactivations: 1000
                  Successful gateway initiated deactivations: 1000
                  Data plane global statistics:
                  Source address violation packets:      0
                  Source address violation bytes:        0
                  Total packets rcvd with non-existent TEIDs: 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

```

show unified-edge ggsn-pgw status preemption-list

Syntax	<pre>show unified-edge ggsn-pgw status preemption-list <brief detail> <fpc-slot fpc-slot> <gateway gateway> <pic-slot pic-slot></pre>
Release Information	<p>Command introduced in Junos OS Mobility Release 11.2W.</p> <p>gateway option introduced in Junos OS Mobility Release 11.4W.</p>
Description	<p>Display the preemption list for guaranteed bit rate (GBR) and non-GBR bearers for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then information for all GGSNs and P-GWs is displayed.</p>
	<div>  <p>NOTE:</p> <ul style="list-style-type: none"> In load conditions, to accommodate higher-priority bearers, lower-priority bearers are preempted. This list displays the number of bearers in each candidate priority level for preemption. This command displays a preemption list only if preemption is enabled on the GGSN or P-GW. </div>
Options	<p>none—(Same as brief) Display the preemption list information in brief.</p> <p>brief detail —(Optional) Display the specified level of output.</p> <p>fpc-slot fpc-slot—(Optional) Display the preemption list information for the specified Flexible PIC Concentrator (FPC) slot number. You must specify a PIC slot number along with an FPC slot number.</p> <p>gateway—(Optional) Display the preemption list information for the specified GGSN or P-GW.</p> <p>pic-slot pic-slot—(Optional) Display the status information for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> show unified-edge ggsn-pgw status on page 1091
List of Sample Output	<p>show unified-edge ggsn-pgw status preemption-list brief on page 1178</p> <p>show unified-edge ggsn-pgw status preemption-list detail on page 1178</p>

Output Fields Table 92 on page 1178 lists the output fields for the **show unified-edge ggsn-pgw status preemption-list** command. Output fields are listed in the approximate order in which they appear.

Table 92: show unified-edge ggsn-pgw status preemption-list Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of GGSN or P-GW.	All levels
FPC Slot	FPC slot number of the interface for which the preemption list information is displayed.	detail
PIC Slot	PIC slot number of the FPC for which the preemption list information is displayed.	detail
Priority Level	<p>Priority of the call that was set up: 1 is the highest and 15 is the lowest. For each priority level, the following information is displayed:</p> <ul style="list-style-type: none"> • GBR—Number of GBR bearers for the corresponding priority level. • NON-GBR—Number of GBR bearers for the corresponding priority level. 	All levels

Sample Output

```
show unified-edge ggsn-pgw status preemption-list brief
user@host> show unified-edge ggsn-pgw status preemption-list brief
Gateway: PGW
```

		GBR	NON-GBR
Priority Level 1	:	0	1
Priority Level 2	:	0	11
Priority Level 3	:	0	0
Priority Level 4	:	0	0
Priority Level 5	:	0	0
Priority Level 6	:	0	0
Priority Level 7	:	0	0
Priority Level 8	:	0	0
Priority Level 9	:	0	0
Priority Level 10	:	0	0
Priority Level 11	:	0	0
Priority Level 12	:	0	0
Priority Level 13	:	0	0
Priority Level 14	:	0	0
Priority Level 15	:	0	0

```
show unified-edge ggsn-pgw status preemption-list detail
user@host> show unified-edge ggsn-pgw status preemption-list detail
Gateway: PGW
```

Preemption List status:

FPC SLOT: 0 PIC SLOT: 0

		GBR	NON-GBR
Priority Level 1	:	0	0
Priority Level 2	:	0	6

Priority Level 3	:	0	0
Priority Level 4	:	0	0
Priority Level 5	:	0	0
Priority Level 6	:	0	0
Priority Level 7	:	0	0
Priority Level 8	:	0	0
Priority Level 9	:	0	0
Priority Level 10	:	0	0
Priority Level 11	:	0	0
Priority Level 12	:	0	0
Priority Level 13	:	0	0
Priority Level 14	:	0	0
Priority Level 15	:	0	0

Preemption List status:

FPC SLOT: 0 PIC SLOT: 1

		GBR	NON-GBR
Priority Level 1	:	0	0
Priority Level 2	:	0	0
Priority Level 3	:	0	0
Priority Level 4	:	0	0
Priority Level 5	:	0	0
Priority Level 6	:	0	0
Priority Level 7	:	0	0
Priority Level 8	:	0	0
Priority Level 9	:	0	0
Priority Level 10	:	0	0
Priority Level 11	:	0	0
Priority Level 12	:	0	0
Priority Level 13	:	0	0
Priority Level 14	:	0	0
Priority Level 15	:	0	0

[...output truncated...]

show unified-edge sgw status preemption-list

Syntax `show unified-edge sgw status preemption-list`
 `<brief | detail>`
 `<fpc-slot fpc-slot>`
 `<gateway gateway>`
 `<pic-slot pic-slot>`

Release Information Command introduced in Junos OS Mobility Release 11.4W.

Description Display the preemption list for guaranteed bit rate (GBR) and non-GBR bearers in the Serving Gateways (S-GWs). If a gateway name is not specified, then the preemption list for all S-GWs is displayed.



NOTE:

- In load conditions, to accommodate higher-priority bearers, lower-priority bearers are preempted. This list displays the number of bearers in each candidate priority level for preemption.
 - This command displays a preemption list only if preemption is enabled on the S-GW.
-

Options `none`—(Same as brief) Display the preemption list information in brief.

`brief | detail` —(Optional) Display the specified level of output.

`fpc-slot fpc-slot`—(Optional) Display the preemption list information for the specified Flexible PIC Concentrator (FPC) slot number. You must specify a PIC slot number along with an FPC slot number.

`gateway gateway`—(Optional) Display the preemption list for the specified gateway.

`pic-slot pic-slot`—(Optional) Display the status information for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

Required Privilege Level view

Related Documentation • [show unified-edge sgw status on page 1295](#)

List of Sample Output [show unified-edge ggsn-pgw status preemption-list brief on page 1181](#)
 [show unified-edge ggsn-pgw status preemption-list detail on page 1181](#)

Output Fields [Table 93 on page 1181](#) lists the output fields for the `show unified-edge sgw status preemption-list` command. Output fields are listed in the approximate order in which they appear.

Table 93: show unified-edge sgw status preemption-list Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the S-GW.	All levels
FPC Slot	FPC slot number of the interface for which the preemption list information is displayed.	detail
PIC Slot	PIC slot number of the FPC for which the preemption list information is displayed.	detail
Priority Level	<p>Priority of the call that was set up: 1 is the highest and 15 is the lowest. For each priority level, the following information is displayed:</p> <ul style="list-style-type: none"> • GBR—Number of GBR bearers for the corresponding priority level. • NON-GBR—Number of GBR bearers for the corresponding priority level. 	All levels

Sample Output

```
show unified-edge ggsn-pgw status preemption-list brief
user@host> show unified-edge ggsn-pgw status preemption-list brief
Gateway: SGW
```

		GBR	NON-GBR
Priority Level 1	:	0	0
Priority Level 2	:	0	0
Priority Level 3	:	0	0
Priority Level 4	:	0	0
Priority Level 5	:	1034	0
Priority Level 6	:	0	1000
Priority Level 7	:	0	0
Priority Level 8	:	0	0
Priority Level 9	:	1000	0
Priority Level 10	:	0	1060
Priority Level 11	:	0	0
Priority Level 12	:	0	0
Priority Level 13	:	0	0
Priority Level 14	:	0	0
Priority Level 15	:	0	0

```
show unified-edge ggsn-pgw status preemption-list detail
user@host> show unified-edge ggsn-pgw status preemption-list detail
Gateway: SGW
```

Preemption List status:

FPC SLOT: 3 PIC SLOT: 0

		GBR	NON-GBR
Priority Level 1	:	0	0
Priority Level 2	:	0	0
Priority Level 3	:	0	0
Priority Level 4	:	0	0
Priority Level 5	:	1034	0
Priority Level 6	:	0	1000

Priority Level 7	:	0	0
Priority Level 8	:	0	0
Priority Level 9	:	1000	0
Priority Level 10	:	0	1060
Priority Level 11	:	0	0
Priority Level 12	:	0	0
Priority Level 13	:	0	0
Priority Level 14	:	0	0
Priority Level 15	:	0	0

CHAPTER 34

Exception Handling Operational Commands

clear unified-edge ggsn-pgw ip-reassembly statistics

Syntax	<code>clear unified-edge ggsn-pgw ip-reassembly statistics</code> <code><fpc-slot <i>fpc-slot</i>></code> <code><gateway <i>gateway</i>></code> <code><inet></code> <code><pic-slot <i>pic-slot</i>></code>
Release Information	Command introduced in Junos OS Mobility Release 11.2W. gateway option introduced in Junos OS Mobility Release 11.4W.
Description	Clear the IP reassembly statistics for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then statistics for all GGSNs and P-GWs are cleared.
Options	none —Clear the IP reassembly statistics for all GGSNs and P-GWs. fpc-slot <i>fpc-slot</i> pic-slot <i>pic-slot</i> —(Optional) Clear the IP reassembly statistics for the specified Flexible PIC Concentrator (FPC) and PIC slot numbers. gateway —(Optional) Clear the IP reassembly statistics for all the services PICs in the specified GGSN or P-GW. inet —(Optional) Clear the IP reassembly for IPv4 packets.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show unified-edge ggsn-pgw ip-reassembly statistics on page 1186
List of Sample Output	clear unified-edge ggsn-pgw ip-reassembly statistics on page 1184
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

<code>clear unified-edge ggsn-pgw ip-reassembly statistics</code>	<code>user@host> clear unified-edge ggsn-pgw ip-reassembly statistics</code> Cleared IP re-assembly statistics
---	--

clear unified-edge sgw ip-reassembly statistics

Syntax	clear unified-edge sgw ip-reassembly statistics <fpc-slot <i>fpc-slot</i> > <gateway <i>gateway</i> > <inet> <pic-slot <i>pic-slot</i> >
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Clear the IP reassembly statistics for one or more Serving Gateways (S-GWs). If a gateway name is not specified, then statistics for all S-GWs are cleared.
Options	<p>none—Clear the IP reassembly statistics for all S-GWs.</p> <p>fpc-slot <i>fpc-slot</i> pic-slot <i>pic-slot</i>—(Optional) Clear the IP reassembly statistics for the specified Flexible PIC Concentrator (FPC) and PIC slot numbers.</p> <p>gateway—(Optional) Clear the IP reassembly statistics for all the services PICs in the specified gateway.</p> <p>inet—(Optional) Clear the IP reassembly statistics for IPv4 packets.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show unified-edge sgw ip-reassembly statistics on page 1189
List of Sample Output	clear unified-edge sgw ip-reassembly statistics on page 1185
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
clear unified-edge sgw ip-reassembly statistics
user@host> clear unified-edge sgw ip-reassembly statistics
Cleared IP re-assembly statistics
```

show unified-edge ggsn-pgw ip-reassembly statistics


Syntax	<pre>show unified-edge ggsn-pgw ip-reassembly statistics <brief detail> <fpc-slot fpc-slot> <gateway gateway> <inet> <pic-slot pic-slot></pre>
Release Information	<p>Command introduced in Junos OS Mobility Release 11.2W.</p> <p>gateway option introduced in Junos OS Mobility Release 11.4W.</p>
Description	Display the IP reassembly statistics for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then statistics for all GGSNs and P-GWs are displayed.
Options	<p>none—(Same as brief) Display the IP reassembly statistics for all GGSNs and P-GWs.</p> <p>brief detail—(Optional) Display the specified level of output.</p>
	<div>  <p>NOTE: The brief option displays the aggregated statistics from all the services PICs for each GGSN or P-GW. The detail option displays the statistics for each services PIC separately for each GGSN or P-GW.</p> </div>
	<p>fpc-slot fpc-slot pic-slot pic-slot—(Optional) Display the IP reassembly statistics for the specified Flexible PIC Concentrator (FPC) and PIC slot numbers.</p> <p>gateway—(Optional) Display the IP reassembly statistics for the specified GGSN or P-GW.</p> <p>inet—(Optional) Display the IP reassembly for IPv4 packets.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear unified-edge ggsn-pgw ip-reassembly statistics on page 1184
List of Sample Output	<p>show unified-edge ggsn-pgw ip-reassembly statistics brief on page 1188</p> <p>show unified-edge ggsn-pgw ip-reassembly statistics detail on page 1188</p>
Output Fields	<p>Table 94 on page 1186 lists the output fields for the show unified-edge ggsn-pgw ip-reassembly statistics command. Output fields are listed in the approximate order in which they appear.</p>

Table 94: show unified-edge ggsn-pgw ip-reassembly statistics Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the GGSN or P-GW.	All levels

Table 94: show unified-edge ggsn-pgw ip-reassembly statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
IP Reassembly Statistics		
FPC Slot	FPC slot number for which the statistics are displayed.	detail
PIC slot	PIC slot number for which the statistics are displayed.	detail
First fragments	Number of first fragments.	All levels
Non-first fragments	Number of non-first fragments.	All levels
Total fragments	Total number of fragments.	All levels
Reassembled packets	Total number of reassembled packets. In this case, all fragments of the packets have been received.	All levels
Merged packets	Total number of merged packets. In this case, all the fragments of a packet have been merged into a single packet.	All levels
Packets pending reassembly	Total number of packets pending reassembly.	All levels
Timed out packets	Total number of fragmented packets that exceeded the reassembly timeout.	All levels
Timed out fragments	Total number of fragments that exceeded the reassembly timeout.	All levels
Exceeded maximum packet length	Number of packets dropped because the defragmented packets exceeded the maximum packet size.	All levels
Fragments Dropped		
Invalid Length	Number of fragments of invalid length received.	All levels
Overlap	Number of overlapping fragments received.	All levels
Duplicate	Number of duplicate fragments received.	All levels
No buffers	Number of fragments dropped because the system ran out of the packet buffer.	All levels
Packet limit exceeded	Total number of fragments dropped because the maximum allowed number of fragments was exceeded.	All levels
Total fragments dropped	Total number of fragments dropped.	All levels

Sample Output

```
show unified-edge user@host> show unified-edge ggsn-pgw ip-reassembly statistics brief
ggsn-pgw Gateway: gw1
ip-reassembly IP reassembly statistics:
statistics brief  First fragments:          1
                  Non-first fragments:      1
                  Total fragments:          2
                  Reassembled packets:      1
                  Merged packets:           1
                  Packets pending reassembly: 0
                  Timed out packets:        0
                  Timed out fragments:      0
                  Exceeded maximum packet length:0
                  Fragments Dropped:
                  Invalid length:           0
                  Overlap:                  0
                  Duplicate:                0
                  No buffers:                0
                  Packet limit exceeded:    0
                  Total fragments dropped:   0
```

```
show unified-edge user@host> show unified-edge ggsn-pgw ip-reassembly statistics detail
ggsn-pgw Gateway: gw1
ip-reassembly IP reassembly statistics (FPC 5 PIC 0):
statistics detail First fragments:          1
                  Non-first fragments:      1
                  Total fragments:          2
                  Reassembled packets:      1
                  Merged packets:           1
                  Packets pending reassembly: 0
                  Timed out packets:        0
                  Timed out fragments:      0
                  Exceeded maximum packet length:0
                  Fragments Dropped:
                  Invalid length :           0
                  Overlap :                 0
                  Duplicate :               0
                  No buffers:               0
                  Packet limit exceeded:    0
                  Total fragments dropped:   0
```

show unified-edge sgw ip-reassembly statistics

Syntax `show unified-edge sgw ip-reassembly statistics`
`<brief | detail>`
`<fpc-slot fpc-slot>`
`<gateway gateway>`
`<inet>`
`<pic-slot pic-slot>`

Release Information Command introduced in Junos OS Mobility Release 11.4W.

Description Display the IP reassembly statistics for the one or more Serving Gateways (S-GWs). If a gateway name is not specified, then statistics for all S-GWs are displayed.

Options **none**—(Same as brief) Display the IP reassembly statistics in brief for all S-GWs.
brief | detail—(Optional) Display the specified level of output.



NOTE: The **brief** option displays the aggregated statistics from all the services PICs for each S-GW. The **detail** option displays the statistics for each services PIC separately for each S-GW.

fpc-slot fpc-slot pic-slot pic-slot—(Optional) Display the IP reassembly statistics for the specified Flexible PIC Concentrator (FPC) and PIC slot numbers.

gateway—(Optional) Display the IP reassembly statistics for the specified gateway.

inet—(Optional) Display the IP reassembly statistics for IPv4 packets.

Required Privilege Level view

Related Documentation • [clear unified-edge sgw ip-reassembly statistics on page 1185](#)

List of Sample Output [show unified-edge sgw ip-reassembly statistics brief on page 1191](#)
[show unified-edge sgw ip-reassembly statistics detail on page 1191](#)

Output Fields [Table 95 on page 1189](#) lists the output fields for the **show unified-edge sgw ip-reassembly statistics** command. Output fields are listed in the approximate order in which they appear.

Table 95: show unified-edge sgw ip-reassembly statistics Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the S-GW.	All levels

IP Reassembly Statistics

Table 95: show unified-edge sgw ip-reassembly statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
Gateway	Name of the S-GW.	All levels
FPC Slot	FPC slot number for which the statistics are displayed.	detail
PIC slot	PIC slot number for which the statistics are displayed.	detail
First fragments	Number of first fragments.	All levels
Non-first fragments	Number of non-first fragments.	All levels
Total fragments	Total number of fragments.	All levels
Reassembled packets	Total number of reassembled packets. In this case, all fragments of the packets have been received.	All levels
Merged packets	Total number of merged packets. In this case, all the fragments of a packet have been merged into a single packet.	All levels
Packets pending reassembly	Total number of packets pending reassembly.	All levels
Timed out packets	Total number of fragmented packets that exceeded the reassembly timeout.	All levels
Timed out fragments	Total number of fragments that exceeded the reassembly timeout.	All levels
Exceeded maximum packet length	Number of packets dropped because the defragmented packets exceeded the maximum packet size.	All levels
Fragments Dropped		
Invalid Length	Number of fragments of invalid length received.	All levels
Overlap	Number of overlapping fragments received.	All levels
Duplicate	Number of duplicate fragments received.	All levels
No buffers	Number of fragments dropped because the system ran out of the packet buffer.	All levels
Packet limit exceeded	Total number of fragments dropped because the maximum allowed number of fragments was exceeded.	All levels
Total fragments dropped	Total number of fragments dropped.	All levels

Sample Output

```

show unified-edge sgw user@host> show unified-edge sgw ip-reassembly statistics brief
ip-reassembly Gateway: sgw1
statistics brief IP reassembly statistics:
                  First fragments:      1
                  Non-first fragments:   2
                  Total fragments:      3
                  Reassembled packets:   1
                  Merged packets:       1
                  Packets pending reassembly: 0
                  Timed out packets:     0
                  Timed out fragments:   0
                  Exceeded maximum packet length:0
Fragments Dropped:
                  Invalid length:       0
                  Overlap:              0
                  Duplicate:            0
                  No buffers:           0
                  Packet limit exceeded: 0
                  Total fragments dropped: 0

```

```

show unified-edge sgw user@host> show unified-edge sgw ip-reassembly statistics detail
ip-reassembly Gateway: sgw1
statistics detail IP reassembly statistics (FPC 5 PIC 1):
                  First fragments:      1
                  Non-first fragments:   2
                  Total fragments:      3
                  Reassembled packets:   1
                  Merged packets:       1
                  Packets pending reassembly: 0
                  Timed out packets:     0
                  Timed out fragments:   0
                  Exceeded maximum packet length:0
Fragments Dropped:
                  Invalid length :      0
                  Overlap :            0
                  Duplicate :          0
                  No buffers:          0
                  Packet limit exceeded: 0
                  Total fragments dropped: 0

```


CHAPTER 35

GPRS Tunneling Protocol (GTP) Operational Commands

clear unified-edge ggsn-pgw gtp peer statistics

Syntax	<code>clear unified-edge ggsn-pgw gtp peer statistics gateway gateway remote-address remote-address</code> <code><fpc-slot fpc-slot></code> <code><gtp-all></code> <code><gtp-v0></code> <code><gtp-v1></code> <code><gtp-v2></code> <code><local-address local-address></code> <code><pic-slot pic-slot></code> <code><routing-instance routing-instance></code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Clear the statistics for the GTP peer on the specified gateway GPRS support node (GGSN) or a Packet Data Network Gateway (P-GW).
Options	<p>gateway gateway—Clear the statistics for the specified gateway.</p> <p>remote-address remote-address—Clear the statistics for the peer with the specified remote address.</p> <p>fpc-slot fpc-slot—(Optional) Clear the statistics for the peer on the specified FPC slot.</p> <p>gtp-all—(Optional) Clear the statistics for GTP versions 0, 1, and 2.</p> <p>gtp-v0—(Optional) Clear the GTP version 0 statistics.</p> <p>gtp-v1—(Optional) Clear the GTP version 1 statistics.</p> <p>gtp-v2—(Optional) Clear the GTP version 2 statistics.</p> <p>local-address local-address—(Optional) Clear the statistics for the peer with the specified local IP address.</p> <p>pic-slot slot—(Optional) Clear the statistics for the peer on the specified PIC slot. You must specify an FPC slot number before specifying a PIC slot number.</p> <p>routing-instance routing-instance—(Optional) Clear the statistics for the peer on the specified routing instance.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show unified-edge ggsn-pgw gtp peer statistics on page 1203
List of Sample Output	clear unified-edge ggsn-pgw gtp peer statistics gateway PGW remote-address 122.2.2.2 on page 1195
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
clear unified-edge    user@host> clear unified-edge ggsn-pgw gtp peer statistics gateway PGW remote-address
ggsn-pgw gtp peer    122.2.2.2
statistics gateway    Cleared GTP peer statistics
PGW remote-address
122.2.2.2
```

clear unified-edge ggsn-pgw gtp statistics

Syntax	<code>clear unified-edge ggsn-pgw gtp peer statistics</code> <code><fpc-slot <i>fpc-slot</i>></code> <code><gateway <i>gateway</i>></code> <code><gtp-all></code> <code><gtp-v0></code> <code><gtp-v1></code> <code><gtp-v2></code> <code><pic-slot <i>pic-slot</i>></code>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Clear the global GTP statistics for the specified gateway GPRS support node (GGSN) or a Packet Data Network Gateway (P-GW).
Options	<p>gateway <i>gateway</i>—Clear the statistics for the specified gateway.</p> <p>fpc-slot <i>fpc-slot</i>—(Optional) Clear the statistics for the specified FPC slot.</p> <p>gtp-all—(Optional) Clear the statistics for GTP versions 0, 1, and 2.</p> <p>gtp-v0—(Optional) Clear the GTP version 0 statistics.</p> <p>gtp-v1—(Optional) Clear the GTP version 1 statistics.</p> <p>gtp-v2—(Optional) Clear the GTP version 2 statistics.</p> <p>pic-slot <i>slot</i>—(Optional) Clear the statistics for the peer on the specified PIC slot. You must specify an FPC slot number before specifying a PIC slot number.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show unified-edge ggsn-pgw gtp statistics on page 1211
List of Sample Output	clear unified-edge ggsn-pgw gtp statistics gateway PGW on page 1196
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

<code>clear unified-edge</code>	<code>user@host> clear unified-edge ggsn-pgw gtp statistics gateway PGW</code>
<code>ggsn-pgw gtp</code>	
<code>statistics gateway</code>	Cleared GTP statistics
<code>PGW</code>	

clear unified-edge sgw gtp peer statistics

Syntax	<pre>clear unified-edge sgw gtp peer statistics remote-address <i>remote-address</i> <fpc-slot <i>fpc-slot</i>> <gateway <i>gateway</i>> <local-address <i>local-address</i>> <pic-slot <i>pic-slot</i>> <routing-instance <i>routing-instance</i>></pre>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Clear the statistics for the specified GPRS tunneling protocol (GTP) peer on one or more Serving Gateways (S-GWs). If an S-GW is not specified, then the statistics are cleared for the specified peer on all the S-GWs.
Options	<p>remote-address <i>remote-address</i>—Clear the statistics for the GTP peer with the specified remote address.</p> <p>fpc-slot <i>fpc-slot</i>—(Optional) Clear the statistics for the specified Flexible PIC Concentrator (FPC) slot number.</p> <p>gateway <i>gateway</i>—(Optional) Clear the statistics for peer on the specified S-GW.</p> <p>local-address <i>local-address</i>—(Optional) Clear the statistics for the peer with the specified local IP address.</p> <p>pic-slot <i>pic-slot</i>—(Optional) Clear the statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.</p> <p>routing-instance <i>routing-instance</i>—(Optional) Clear the statistics for the peer on the specified routing instance.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show unified-edge sgw gtp peer statistics on page 1225
List of Sample Output	clear unified-edge sgw gtp peer statistics remote-address 122.2.2.2 on page 1197
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

```
clear unified-edge sgw  user@host> clear unified-edge sgw gtp peer statistics remote-address 122.2.2.2
gtp peer statistics      Cleared GTP Peer statistics
remote-address
122.2.2.2
```

clear unified-edge sgw gtp statistics

Syntax	<code>clear unified-edge sgw gtp statistics</code> <code><fpc-slot <i>fpc-slot</i>></code> <code><gateway <i>gateway</i>></code> <code><pic-slot <i>pic-slot</i>></code>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Clear the global GPRS tunneling protocol (GTP) statistics for the specified Serving Gateway (S-GW).
Options	<p>fpc-slot <i>fpc-slot</i>—(Optional) Clear the GTP statistics for the specified Flexible PIC Concentrator (FPC) slot number.</p> <p>gateway <i>gateway</i>—(Optional) Clear the GTP statistics for the specified S-GW.</p> <p>pic-slot <i>pic-slot</i>—(Optional) Clear the GTP statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show unified-edge sgw gtp statistics on page 1230
List of Sample Output	clear unified-edge sgw gtp statistics gateway SGW on page 1198
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

<code>clear unified-edge sgw gtp statistics gateway SGW</code>	<code>user@host> clear unified-edge sgw gtp statistics gateway SGW</code> Cleared GTP statistics
--	--

show unified-edge ggsn-pgw gtp peer

Syntax `show unified-edge ggsn-pgw gtp peer`
`<detail>`
`<fpc-slot fpc-slot>`
`<gateway gateway>`
`<history>`
`<local-address local-address>`
`<pic-slot pic-slot>`
`<remote-address remote-address>`
`<routing-instance name>`

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Display the information about GTP peers for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then the information for all GGSNs and P-GWs is displayed.

Options **none**—Display the GTP peer information in brief.

detail—(Optional) Display detailed information about GTP peers.

fpc-slot fpc-slot—(Optional) Display the GTP peer information for the specified FPC slot number.

gateway gateway-name—(Optional) Display the GTP peer information for the specified gateway.

history—(Optional) Display the GTP peer information for peers which are no longer present on the gateway.

local-address local-address—(Optional) Display the GTP peer information for the local address of the specified peer on the gateway.

pic-slot pic-slot—(Optional) Display the GTP peer for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

remote-address remote-address—(Optional) Display the GTP peer information for the peer with the specified remote address.

routing-instance routing-instance—(Optional) Display the GTP peer information for the peer on the specified routing instance.



NOTE: If you specify the routing instance, you must also specify the remote address of the peer.

Required Privilege Level view

- Related Documentation**
- [clear unified-edge ggsn-pgw gtp peer statistics on page 1194](#)
 - [show unified-edge ggsn-pgw gtp peer statistics on page 1203](#)

List of Sample Output [show unified-edge ggsn-pgw gtp peer on page 1201](#)
[show unified-edge ggsn-pgw gtp peer detail on page 1201](#)

Output Fields Table 96 on page 1200 lists the output fields for the **show unified-edge ggsn-pgw gtp peer** command. Output fields are listed in the approximate order in which they appear.

Table 96: show unified-edge ggsn-pgw gtp peer Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the GGSN or P-GW.	All levels
Rmt IP Address	Remote IP address of the GTP peer.	All levels
Local IP Address	Local IP address of the GTP peer on the gateway.	All levels
Routing Instance	Routing instance on which the GTP peer is located	All levels
Interface Type	Type of 3GPP interface; for example S5, S8, and so on.	detail
GTP Version	GTP version number.	detail
RCM Registration Done	This parameter is used internally by the gateway.	detail
Is Restart Counter Valid	Indicates whether the restart counter of the peer is valid or not.	detail
Restart Counter Value	Current restart count of the peer.	detail
Sent Restart Counter Value	Restart counter value of the gateway that was sent to the peer.	detail
Control Path N3 Req	Maximum number of times that the S-GW attempts to send a signaling request message to a control peer.	detail
Control Path T3 Timer	Response timeout for GTP signaling request messages to a control peer.	detail
Control Path Echo N3 Req	Maximum number of retries of GTP echo request messages (for path management) to a control peer.	detail
Control Path Echo T3 Timer	Response timeout for GTP echo request messages (for path management) to a control peer.	detail
Control Path Echo Interval	Number of seconds that the GGSN or P-GW waits before sending an echo request message (for path management) to its control peer.	detail
Downlink data notif delay Interval	This field is not relevant for the GGSN or P-GW.	detail

Table 96: show unified-edge ggsn-pgw gtp peer Output Fields (*continued*)

Field Name	Field Description	Level of Output
Is Path Management Enabled (control)	Indicates whether path management is enabled or not for the control plane.	detail
Is CSID Supported	Indicates whether the connection set identifier (CSID) is supported by the peer or not.	detail
Is GTP-C using Short Seq Number	Indicates whether the peer is using the 16-bit sequence number length.	detail
GTP-C Path State	Path state of the GTP control plane: <ul style="list-style-type: none"> • Active—Indicates that echo request messages are being transmitted or received. • Inactive—If path management is enabled, then this peer is inactive. Otherwise, this state should be ignored. 	detail
Data Path Echo N3 Req	Maximum number of retries of GTP echo request messages (for path management) to a data peer.	detail
Data Path Echo T3 Timer	Response timeout for GTP echo request messages (for path management) to a data peer.	detail
Data Path Echo Interval	Number of seconds that the GGSN or P-GW waits before sending an echo request message (for path management) to its data peer.	detail
Is PATH Management Enabled (Data)	Indicates whether path management is enabled or not for the data plane.	detail
GTP-U Path State	Path state of the GTP user plane: <ul style="list-style-type: none"> • Active—Indicates that echo request messages are being transmitted or received. • Inactive—If path management is enabled, then this peer is inactive. Otherwise, this state should be ignored. 	detail

Sample Output

```

show unified-edge ggsn-pgw gtp peer user@host> show unified-edge ggsn-pgw gtp peer
Gateway: PGW2
Rmt IP Address          Local IP Address      Routing-Instance
-----
34.34.34.1              17.1.1.4              0

```

```

show unified-edge ggsn-pgw gtp peer detail user@host> show unified-edge ggsn-pgw gtp peer detail
Peer Detail:
-----
Remote IP Addr          : 34.34.34.1
Local IP Addr           : 17.1.1.4
Routing Instance        : 0
Interface Type           : GTP_INTF_S5

```

```
GTP Version                : 2
RCM Registration Done      : yes
Is Restart Counter Valid   : no
Restart Counter Value      : 0
Sent Restart Counter Value : 2
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 : 70
Downlink data notif delay Interval : 0
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 echo N3 Req      : 8
Data Path echo T3 Timer    : 15
Data Path Echo Interval    : 70
Is PATH Management Enabled (Data) : no
GTP-U Path State           : inactive
```


show unified-edge ggsn-pgw gtp peer statistics

Syntax	<pre>show unified-edge ggsn-pgw gtp peer statistics remote-address <i>remote-address</i> <detail> <fpc-slot <i>fpc-slot</i>> <gateway <i>gateway</i>> <gtp-all> <gtp-v0> <gtp-v1> <gtp-v2> <history> <local-address <i>local-address</i>> <pic-slot <i>pic-slot</i>> <routing-instance <i>routing-instance</i>></pre>
Release Information	<p>Command introduced in Junos OS Mobility Release 11.2W.</p> <p>gateway option introduced in Junos OS Mobility Release 11.4W.</p>
Description	Display the GTP peer statistics for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then the status for all GGSNs and P-GWs is displayed.
Options	<p>remote-address <i>remote-address</i>—Display the GTP peer statistics for the peer with the specified remote address.</p> <p>detail—(Optional) Display detailed statistics about GTP peers.</p> <p>fpc-slot <i>fpc-slot</i>—(Optional) Display the GTP peer statistics for the specified FPC slot number.</p> <p>gateway <i>gateway-name</i>—(Optional) Display the GTP peer statistics for the specified gateway.</p> <p>gtp-all—(Optional) Display the statistics for GTP versions 0, 1, and 2.</p> <p>gtp-v0—(Optional) Display the GTP version 0 statistics.</p> <p>gtp-v1—(Optional) Display the GTP version 1 statistics.</p> <p>gtp-v2—(Optional) Display the GTP version 2 statistics.</p> <p>history—(Optional) Display the GTP peer statistics for peers which are no longer present on the gateway.</p> <p>local-address <i>local-address</i>—(Optional) Display the GTP peer statistics for the local address of the specified peer on the S-GW.</p> <p>pic-slot <i>pic-slot</i>—(Optional) Display the GTP peer statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.</p> <p>routing-instance <i>routing-instance</i>—(Optional) Display the GTP peer statistics for the peer on the specified routing instance.</p>

Required Privilege Level view

- Related Documentation**
- [clear unified-edge ggsn-pgw gtp peer statistics on page 1194](#)
 - [show unified-edge ggsn-pgw gtp peer on page 1199](#)
 - [show unified-edge ggsn-pgw gtp statistics on page 1211](#)

List of Sample Output [show unified-edge ggsn-pgw gtp peer statistics remote-address 17.1.1.1 on page 1204](#)
[show unified-edge ggsn-pgw gtp peer statistics remote-address 17.1.1.1 detail on page 1206](#)

Output Fields See the output fields for the [show unified-edge ggsn-pgw gtp statistics](#) command.

Sample Output

```

show unified-edge user@host> show unified-edge ggsn-pgw gtp peer statistics remote-address 17.1.1.1
ggsn-pgw gtp peer Gateway: PGW2
statistics
remote-address 17.1.1.1
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
  GTP Unknown Version 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            0             0
Total number of bytes                0             0
Redirect messages                    0             0
Echo Request                        0             0
Echo Response                        0             0
Version Not Supported                0             0
Create PDP Context Request           0             0
Create PDP Context Response          0             0
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	0	0
Total number of bytes	0	0
Redirect messages	0	0
Echo Request	0	0
Echo Response	0	0
Version Not Supported	0	0
Create PDP Context Request	0	0
Create PDP Context Response	0	0
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 2 Statistics:

Protocol Error	: 0
Unsupported Messages Received	: 0
T3 Response Timer Expires	: 0

Message Type	Received	Transmitted

Total number of messages	6	6
Total number of bytes	266	162
Redirect messages	0	0
S11 piggyback messages	0	0
S4 piggyback messages	0	0
S5 piggyback messages	0	0
Echo Request	5	0
Echo Response	0	5
Version Not Supported	0	0
Create session request	1	0
Create session response	0	1
Modify bearer request	0	0
Modify bearer response	0	0
Delete session request	0	0
Delete session response	0	0
Create bearer request	0	0
Create bearer response	0	0
Update bearer request	0	0
Update bearer response	0	0
Delete bearer request	0	0
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
Release Access Bearer request	0	
0		
Release Access Bearer response	0	
0		

Suspend Notification	0	0
Suspend Acknowledge	0	0
Resume Notification	0	0
Resume Acknowledge	0	0
Create Indirect Data Forward Tunnel Request	0	0
Create Indirect Data Forward Tunnel Response	0	0
Delete Indirect Data Forward Tunnel Request	0	0
Delete Indirect Data Forward Tunnel Response	0	0
Downlink Data Notification	0	0
Downlink Data Notification ack	0	0
Downlink Data Notification fail	0	0
Stop paging indication	0	0

Error Indication Statistics:

Version	Received	Transmitted

GTPv0	0	0
GTPv1	0	0

```

show unified-edge user@host> show unified-edge ggsn-pgw gtp peer statistics remote-address 17.1.1.1 detail
ggsn-pgw gtp peer Gateway: PGW2
statistics
remote-address 17.1.1.1
detail

```

```

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
GTP Unknown Version 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	0	0
Total number of bytes	0	0
Redirect messages	0	0
Echo Request	0	0
Echo Response	0	0
Version Not Supported	0	0
Create PDP Context Request	0	0
Create PDP Context Response	0	0
Update PDP Context Request	0	0
Update PDP Context Response	0	0
Delete PDP Context Request	0	0
Delete PDP Context Response	0	0

Cause Code	Received	Transmitted

Request Accepted	0	0

Non Existent	0	0
Invalid Message Format	0	0
IMSI Not Known	0	0
MS is GPRS Detached	0	0
MS is not GPRS Response	0	0
MS Refuses	0	0
Version Not Supported	0	0
No Resource Available	0	0
Service Not Supported	0	0
Mandatory IE Incorrect	0	0
Mandatory IE Missing	0	0
Optional IE Incorrect	0	0
System Failure	0	0
Roaming Restriction	0	0
P-TMSI Signature Mismatch	0	0
GPRS Connection Suspended	0	0
Authentication Failure	0	0
User Authentication Failed	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	0	0
Total number of bytes	0	0
Redirect messages	0	0
Echo Request	0	0
Echo Response	0	0
Version Not Supported	0	0
Create PDP Context Request	0	0
Create PDP Context Response	0	0
Update PDP Context Request	0	0
Update PDP Context Response	0	0
Delete PDP Context Request	0	0
Delete PDP Context Response	0	0

Cause Code	Received	Transmitted

Request Accepted	0	0
Non Existent	0	0
Invalid Message Format	0	0
IMSI Not Known	0	0
MS is GPRS Detached	0	0
MS is not GPRS Response	0	0
MS Refuses	0	0
Version Not Supported	0	0
No Resource Available	0	0
Service Not Supported	0	0
Mandatory IE Incorrect	0	0
Mandatory IE Missing	0	0
Optional IE Incorrect	0	0
System Failure	0	0
Roaming Restriction	0	0
P-TMSI Signature Mismatch	0	0
GPRS Connection Suspended	0	0

Authentication Failure	0	0
User Authentication Failed	0	0
Context not found	0	0
All dynamic PDP addresses are occupied	0	0
No memory is available	0	0
Relocation failure	0	0
Unknown mandatory extension header	0	0
Semantic error in the TFT operation	0	0
Syntactic error in the TFT operation	0	0
Semantic errors in packet filter(s)	0	0
Syntactic errors in packet filter(s)	0	0
Missing or unknown APN	0	0
Unknown PDP address or PDP type	0	0
PDP context without TFT already activated	0	0

GTP Version 2 Statistics:

Protocol Error	: 0
Unsupported Messages Received	: 0
T3 Response Timer Expires	: 0

Message Type	Received	Transmitted

Total number of messages	7	7
Total number of bytes	279	175
Redirect messages	0	0
S11 piggyback messages	0	0
S4 piggyback messages	0	0
S5 piggyback messages	0	0
Echo Request	6	0
Echo Response	0	6
Version Not Supported	0	0
Create session request	1	0
Create session response	0	1
Modify bearer request	0	0
Modify bearer response	0	0
Delete session request	0	0
Delete session response	0	0
Create bearer request	0	0
Create bearer response	0	0
Update bearer request	0	0
Update bearer response	0	0
Delete bearer request	0	0
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
Release Access Bearer request	0	
0		
Release Access Bearer response	0	
0		

Suspend Notification	0	0
Suspend Acknowledge	0	0
Resume Notification	0	0
Resume Acknowledge	0	0
Create Indirect Data Forward Tunnel Request	0	0
Create Indirect Data Forward Tunnel Response	0	0
Delete Indirect Data Forward Tunnel Request	0	0
Delete Indirect Data Forward Tunnel Response	0	0
Downlink Data Notification	0	0
Downlink Data Notification ack	0	0
Downlink Data Notification fail	0	0
Stop paging indication	0	0

Cause Code	Received	Transmitted

Request accepted	0	1
Request accepted partially	0	0
New PDN type due to network preference	0	0
New PDN type due to single address bearer only	0	0
Local Detach	0	0
Complete Detach	0	0
RAT changed from 3GPP to Non 3GPP	0	0
ISR Deactivated	0	0
Error Indication from RNC Enodeb	0	0
Context Not Found	0	0
Invalid Message Format	0	0
Version not supported by next peer	0	0
Invalid length	0	0
Service not supported	0	0
Mandatory IE incorrect	0	0
Mandatory IE missing	0	0
Optional IE incorrect	0	0
System failure	0	0
No resources available	0	0
Semantic error in the TFT operation	0	0
Syntactic error in the TFT operation	0	0
Semantic errors in packet filter(s)	0	0
Syntactic errors in packet filter(s)	0	0
Missing or unknown APN	0	0
Unexpected repeated IE	0	0
GRE key not found	0	0
Reallocation failure	0	0
Denied in RAT	0	0
Preferred PDN type not supported	0	0
All dynamic addresses are occupied	0	0
UE context without TFT already activated	0	0
Protocol type not supported	0	0
UE not responding	0	0
UE refuses	0	0
Service denied	0	0
Unable to page UE	0	0
No memory available	0	0
User authentication failed	0	0
APN access denied - no subscription	0	0
Request rejected	0	0
P-TMSI Signature Mismatch	0	0
IMSI Not Known	0	0
Semantic Error in the TAD Operation	0	0
Syntactic Error in the TAD Operation	0	0
Reserved Message Value Received	0	0

Rmt Peer Not Responding	0	0
Collision with Network Initiated Request	0	0
Unable to Page UE due to Suspension	0	0
Conditional IE Missing	0	0
APN Restriction Type Incompatible	0	0
Invalid Total len	0	0
Data Forwarding Not Supported	0	0
Invalid Reply from Rmt Peer	0	0
Invalid Peer	0	0
Unknown	0	0

Error Indication Statistics:

Version	Received	Transmitted

GTPv0	0	0
GTPv1	0	0

show unified-edge ggsn-pgw gtp statistics

Syntax	<pre>show unified-edge ggsn-pgw gtp statistics <detail> <fpc-slot fpc-slot> <gateway gateway> <gtp-all> <gtp-error-ind> <gtp-v0> <gtp-v1> <gtp-v2> <pic-slot pic-slot></pre>
Release Information	Statement introduced in Junos OS Mobility Release 11.2W.
Description	Display the global GTP statistics for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then the status for all GGSNs and P-GWs is displayed.
Options	<p>none—Display the GTP statistics in brief.</p> <p>detail—(Optional) Display the GTP statistics with the GTP cause statistics included.</p> <p>fpc-slot fpc-slot—(Optional) Display the GTP statistics for the specified FPC slot number.</p> <p>gateway gateway-name—(Optional) Display the GTP statistics for the specified gateway.</p> <p>gtp-all—(Optional) Display the statistics for GTP versions 0, 1, and 2 including the error indication statistics.</p> <p>gtp-error-ind—(Optional) Display the GTP error indication statistics.</p> <p>gtp-v0—(Optional) Display the GTP version 0 statistics.</p> <p>gtp-v1—(Optional) Display the GTP version 1 statistics.</p> <p>gtp-v2—(Optional) Display the GTP version 2 statistics.</p> <p>pic-slot pic-slot—(Optional) Display the GTP statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear unified-edge ggsn-pgw gtp statistics on page 1196 • show unified-edge ggsn-pgw gtp peer statistics on page 1203
List of Sample Output	<p>show unified-edge ggsn-pgw gtp statistics on page 1214</p> <p>show unified-edge ggsn-pgw gtp statistics detail on page 1216</p>
Output Fields	Table 97 on page 1212 lists the output fields for the show unified-edge sgw gtp statistics command. Output fields are listed in the approximate order in which they appear.

Table 97: show unified-edge sgw gtp statistics Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the GGSN or P-GW.	All levels
Global Packet Statistics		
Received Packets Dropped	Total number of packets received by the GGSN or P-GW that were dropped.	All levels
Packet Allocation Fail	Number of times that packet allocation failed.	All levels
Packet Send Fail	Number of times that packet sending failed.	All levels
IP Version Error Received	Number of packets with an unsupported IP version.	All levels
IP Protocol Error Received	Number of non-UDP IP packets received.	All levels
GTP Port Error Received	Number of packets received on a unknown GTP port number.	All levels
GTP Unknown Version Received	Number of GTP packets with an incorrect GTP version.	All levels
Packet Length Error Received	Number of GTP packets with an incorrect length in the IP or UDP header.	All levels
Unknown Messages Received	Number of GTP messages received that are not recognized by the gateway.	All levels
GTP Version 0 Statistics		
Protocol Error	Number of messages received that had a protocol error. This counter is incremented if a message with an invalid or unknown GTP message type is received.	All levels
Unsupported Messages Received	Number of unsupported messages received. This counter is incremented if the message is invalid for the interface on which the message is received.	All levels
T3 Response Timer Expires	Number of messages for which the T3 response timer elapsed.	All levels
Message Type	Type of the GTP message; for example, Echo Request or Create PDP Context Request .	All levels
Received	Number of GTP messages received corresponding to the message type.	All levels
Transmitted	Number of GTP messages transmitted corresponding to the message type.	All levels
Cause Code	GTP cause codes; for example, Request accepted or Invalid Message Format .	detail

Table 97: show unified-edge sgw gtp statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
Received	Number of GTP messages received corresponding to the GTP cause code.	detail
Transmitted	Number of GTP messages transmitted corresponding to the GTP cause code.	detail
GTP Version 1 Statistics		
Protocol Error	Number of messages received that had a protocol error. This counter is incremented if a message with an invalid or unknown GTP message type is received.	All levels
Unsupported Messages Received	Number of unsupported messages received. This counter is incremented if the message is invalid for the interface on which the message is received.	All levels
T3 Response Timer Expires	Number of messages for which the T3 response timer elapsed.	All levels
Message Type	Type of the GTP message; for example, Echo Request or Create PDP Context Request .	All levels
Received	Number of GTP messages received corresponding to the message type.	All levels
Transmitted	Number of GTP messages transmitted corresponding to the message type.	All levels
Cause Code	GTP cause codes; for example, Request accepted or Invalid Message Format .	detail
Received	Number of GTP messages received corresponding to the GTP cause code.	detail
Transmitted	Number of GTP messages transmitted corresponding to the GTP cause code.	detail
GTP Version 2 Statistics		
Protocol Error	Number of messages received that had a protocol error. This counter is incremented if a message with an invalid or unknown GTP message type is received.	All levels
Unsupported Messages Received	Number of unsupported messages received. This counter is incremented if the message is invalid for the interface on which the message is received.	All levels
T3 Response Timer Expires	Number of messages for which the T3 response timer elapsed.	All levels
Message Type	Type of the GTP message; for example, Echo Request or Create PDP Context Request .	All levels

Table 97: show unified-edge sgw gtp statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
Received	Number of GTP messages received corresponding to the message type.	All levels
Transmitted	Number of GTP messages transmitted corresponding to the message type.	All levels
Cause Code	GTP cause codes; for example, Request accepted or Invalid Message Format .	detail
Received	Number of GTP messages received corresponding to the GTP cause code.	detail
Transmitted	Number of GTP messages transmitted corresponding to the GTP cause code.	detail
Error Indication Statistics		
Version	GTP version (GTP version 0 and GTP version 1) for which the error indication statistics are displayed.	All levels
Received	Number of error indication messages received, corresponding to the GTP version.	All levels
Transmitted	Number of error indication messages transmitted, corresponding to the GTP version.	All levels

Sample Output

```
show unified-edge ggsn-pgw gtp statistics
user@host> show unified-edge ggsn-pgw gtp statistics
Gateway: PGW2
```

```
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
GTP Unknown Version 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	0	0
Total number of bytes	0	0

Redirect messages	0	0
Echo Request	0	0
Echo Response	0	0
Version Not Supported	0	0
Create PDP Context Request	0	0
Create PDP Context Response	0	0
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	0	0
Total number of bytes	0	0
Redirect messages	0	0
Echo Request	0	0
Echo Response	0	0
Version Not Supported	0	0
Create PDP Context Request	0	0
Create PDP Context Response	0	0
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 2 Statistics:

Protocol Error	: 0
Unsupported Messages Received	: 0
T3 Response Timer Expires	: 0

Message Type	Received	Transmitted
Total number of messages	9	9
Total number of bytes	269	201
Redirect messages	0	0
S11 piggyback messages	0	0
S4 piggyback messages	0	0
S5 piggyback messages	0	0
Echo Request	8	0
Echo Response	0	8
Version Not Supported	0	0
Create session request	1	0
Create session response	0	1
Modify bearer request	0	0
Modify bearer response	0	0
Delete session request	0	0
Delete session response	0	0
Create bearer request	0	0
Create bearer response	0	0
Update bearer request	0	0
Update bearer response	0	0

Delete bearer request	0	0
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
Release Access Bearer request	0	
0		
Release Access Bearer response	0	
0		
Suspend Notification	0	0
Suspend Acknowledge	0	0
Resume Notification	0	0
Resume Acknowledge	0	0
Create Indirect Data Forward Tunnel Request	0	0
Create Indirect Data Forward Tunnel Response	0	0
Delete Indirect Data Forward Tunnel Request	0	0
Delete Indirect Data Forward Tunnel Response	0	0
Downlink Data Notification	0	0
Downlink Data Notification ack	0	0
Downlink Data Notification fail	0	0
Stop paging indication	0	0

Error Indication Statistics:

Version	Received	Transmitted
-----	-----	-----
GTPv0	0	0
GTPv1	0	0

show unified-edge user@host> show unified-edge ggsn-pgw gtp statistics detail
ggsn-pgw gtp Gateway: PGW2
statistics detail

```
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
GTP Unknown Version 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	0	0
Total number of bytes	0	0
Redirect messages	0	0
Echo Request	0	0
Echo Response	0	0
Version Not Supported	0	0
Create PDP Context Request	0	0
Create PDP Context Response	0	0
Update PDP Context Request	0	0
Update PDP Context Response	0	0
Delete PDP Context Request	0	0
Delete PDP Context Response	0	0

Cause Code	Received	Transmitted

Request Accepted	0	0
Non Existent	0	0
Invalid Message Format	0	0
IMSI Not Known	0	0
MS is GPRS Detached	0	0
MS is not GPRS Response	0	0
MS Refuses	0	0
Version Not Supported	0	0
No Resource Available	0	0
Service Not Supported	0	0
Mandatory IE Incorrect	0	0
Mandatory IE Missing	0	0
Optional IE Incorrect	0	0
System Failure	0	0
Roaming Restriction	0	0
P-TMSI Signature Mismatch	0	0
GPRS Connection Suspended	0	0
Authentication Failure	0	0
User Authentication Failed	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	0	0
Total number of bytes	0	0
Redirect messages	0	0
Echo Request	0	0
Echo Response	0	0
Version Not Supported	0	0
Create PDP Context Request	0	0
Create PDP Context Response	0	0
Update PDP Context Request	0	0
Update PDP Context Response	0	0
Delete PDP Context Request	0	0
Delete PDP Context Response	0	0

Cause Code	Received	Transmitted
------------	----------	-------------

Request Accepted	0	0
Non Existent	0	0
Invalid Message Format	0	0
IMSI Not Known	0	0
MS is GPRS Detached	0	0
MS is not GPRS Response	0	0
MS Refuses	0	0
Version Not Supported	0	0
No Resource Available	0	0
Service Not Supported	0	0
Mandatory IE Incorrect	0	0
Mandatory IE Missing	0	0
Optional IE Incorrect	0	0
System Failure	0	0
Roaming Restriction	0	0
P-TMSI Signature Mismatch	0	0
GPRS Connection Suspended	0	0
Authentication Failure	0	0
User Authentication Failed	0	0
Context not found	0	0
All dynamic PDP addresses are occupied	0	0
No memory is available	0	0
Relocation failure	0	0
Unknown mandatory extension header	0	0
Semantic error in the TFT operation	0	0
Syntactic error in the TFT operation	0	0
Semantic errors in packet filter(s)	0	0
Syntactic errors in packet filter(s)	0	0
Missing or unknown APN	0	0
Unknown PDP address or PDP type	0	0
PDP context without TFT already activated	0	0

GTP Version 2 Statistics:

Protocol Error	: 0
Unsupported Messages Received	: 0
T3 Response Timer Expires	: 0

Message Type	Received	Transmitted
Total number of messages	16	16
Total number of bytes	332	292
Redirect messages	0	0
S11 piggyback messages	0	0
S4 piggyback messages	0	0
S5 piggyback messages	0	0
Echo Request	15	0
Echo Response	0	15
Version Not Supported	0	0
Create session request	1	0
Create session response	0	1
Modify bearer request	0	0
Modify bearer response	0	0
Delete session request	0	0
Delete session response	0	0
Create bearer request	0	0
Create bearer response	0	0
Update bearer request	0	0
Update bearer response	0	0

Delete bearer request	0	0
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
Release Access Bearer request	0	
0		
Release Access Bearer response	0	
0		
Suspend Notification	0	0
Suspend Acknowledge	0	0
Resume Notification	0	0
Resume Acknowledge	0	0
Create Indirect Data Forward Tunnel Request	0	0
Create Indirect Data Forward Tunnel Response	0	0
Delete Indirect Data Forward Tunnel Request	0	0
Delete Indirect Data Forward Tunnel Response	0	0
Downlink Data Notification	0	0
Downlink Data Notification ack	0	0
Downlink Data Notification fail	0	0
Stop paging indication	0	0

Cause Code	Received	Transmitted

Request accepted	0	1
Request accepted partially	0	0
New PDN type due to network preference	0	0
New PDN type due to single address bearer only	0	0
Local Detach	0	0
Complete Detach	0	0
RAT changed from 3GPP to Non 3GPP	0	0
ISR Deactivated	0	0
Error Indication from RNC Enodeb	0	0
Context Not Found	0	0
Invalid Message Format	0	0
Version not supported by next peer	0	0
Invalid length	0	0
Service not supported	0	0
Mandatory IE incorrect	0	0
Mandatory IE missing	0	0
Optional IE incorrect	0	0
System failure	0	0
No resources available	0	0
Semantic error in the TFT operation	0	0
Syntactic error in the TFT operation	0	0
Semantic errors in packet filter(s)	0	0
Syntactic errors in packet filter(s)	0	0
Missing or unknown APN	0	0
Unexpected repeated IE	0	0
GRE key not found	0	0
Reallocation failure	0	0

Denied in RAT	0	0
Preferred PDN type not supported	0	0
All dynamic addresses are occupied	0	0
UE context without TFT already activated	0	0
Protocol type not supported	0	0
UE not responding	0	0
UE refuses	0	0
Service denied	0	0
Unable to page UE	0	0
No memory available	0	0
User authentication failed	0	0
APN access denied - no subscription	0	0
Request rejected	0	0
P-TMSI Signature Mismatch	0	0
IMSI Not Known	0	0
Semantic Error in the TAD Operation	0	0
Syntactic Error in the TAD Operation	0	0
Reserved Message Value Received	0	0
Rmt Peer Not Responding	0	0
Collision with Network Initiated Request	0	0
Unable to Page UE due to Suspension	0	0
Conditional IE Missing	0	0
APN Restriction Type Incompatible	0	0
Invalid Total len	0	0
Data Forwarding Not Supported	0	0
Invalid Reply from Rmt Peer	0	0
Invalid Peer	0	0
Unknown	0	0

Error Indication Statistics:

Version	Received	Transmitted

GTPv0	0	0
GTPv1	0	0

show unified-edge sgw gtp peer

Syntax `show unified-edge sgw gtp peer`
 `<detail>`
 `<fpc-slot fpc-slot>`
 `<gateway gateway>`
 `<local-address local-address>`
 `<pic-slot pic-slot>`
 `<remote-address remote-address>`
 `<routing-instance routing-instance>`

Release Information Command introduced in Junos OS Mobility Release 11.4W.

Description Display the information about GTP peers for one or more Serving Gateways (S-GWs). If a gateway is not specified, then the information for all S-GWs is displayed.

Options **none**—Display the GTP peer information in brief.

detail—(Optional) Display detailed information about GTP peers.

fpc-slot fpc-slot—(Optional) Display the GTP peer information for the specified FPC slot number.

gateway gateway-name—(Optional) Display the GTP peer information for the specified gateway.

local-address local-address—(Optional) Display the GTP peer information for the local address of the specified peer on the S-GW.

pic-slot pic-slot—(Optional) Display the GTP peer information for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

remote-address remote-address—(Optional) Display the GTP peer information for the peer with the specified remote address.

routing-instance routing-instance—(Optional) Display the GTP information for the peer on the specified routing instance.



NOTE: If you specify the routing instance, you must also specify the remote address of the peer.

Required Privilege Level view

Related Documentation • [clear unified-edge sgw gtp peer statistics on page 1197](#)
 • [show unified-edge sgw gtp peer statistics on page 1225](#)

List of Sample Output [show unified-edge sgw gtp peer on page 1223](#)
[show unified-edge sgw gtp peer detail on page 1223](#)

Output Fields [Table 98 on page 1222](#) lists the output fields for the **show unified-edge sgw gtp peer** command. Output fields are listed in the approximate order in which they appear.

Table 98: show unified-edge sgw gtp peer Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the S-GW for which the GTP peer information is displayed.	All levels
Rmt IP Address	Remote IP address of the GTP peer.	All levels
Local IP Address	Local IP address of the GTP peer on the S-GW.	All levels
Routing Instance	Routing instance on which the GTP peer is located.	All levels
Interface Type	Type of 3GPP interface; for example S11, S4, and so on.	detail
GTP Version	GTP version number.	detail
RCM Registration Done	This parameter is used internally by the S-GW.	detail
Is Restart Counter Valid	Indicates whether the restart counter of the peer is valid or not.	detail
Restart Counter Value	Current restart count of the peer.	detail
Sent Restart Counter Value	Restart counter value of the S-GW that was sent to the peer.	detail
Control Path N3 Req	Maximum number of times that the S-GW attempts to send a signaling request message to a control peer.	detail
Control Path T3 Timer	Response timeout for GTP signaling request messages to a control peer.	detail
Control Path Echo N3 Req	Maximum number of retries of GTP echo request messages (for path management) to a control peer.	detail
Control Path Echo T3 Timer	Response timeout for GTP echo request messages (for path management) to a control peer.	detail
Control Path Echo Interval	Number of seconds that the S-GW waits before sending an echo request message (for path management) to its control peer (MME, S4-SGSN, or P-GW).	detail
Downlink data notif delay Interval	Downlink data notification delay received from the MME.	detail
Is Path Management Enabled (control)	Indicates whether path management is enabled or not for the control plane.	detail
Is CSID Supported	Indicates whether the connection set identifier (CSID) is supported by peer or not.	detail

Table 98: show unified-edge sgw gtp peer Output Fields (*continued*)

Field Name	Field Description	Level of Output
Is GTP-C using Short Seq Number	Indicates whether the peer is using the 16-bit-sequence number length.	detail
GTP-C Path State	Path state of the GTP control plane: <ul style="list-style-type: none"> • Active—Indicates that echo request messages are being transmitted or received. • Inactive—If path management is enabled, then this peer is inactive. Otherwise, this state should be ignored. 	detail
Data Path Echo N3 Req	Maximum number of retries of GTP echo request messages (for path management) to a data peer.	detail
Data Path Echo T3 Timer	Response timeout for GTP echo request messages (for path management) to a data peer.	detail
Data Path Echo Interval	Number of seconds that the S-GW waits before sending an echo request message (for path management) to its data peer.	detail
Is PATH Management Enabled (Data)	Indicates whether path management is enabled or not for the data plane.	detail
GTP-U Path State	Path state of the GTP user plane: <ul style="list-style-type: none"> • Active—Indicates that echo request messages are being transmitted or received. • Inactive—If path management is enabled, then this peer is inactive. Otherwise, this state should be ignored. 	detail

Sample Output

```

show unified-edge sgw gtp peer
user@host> show unified-edge sgw gtp peer
Gateway: SGW
Rmt IP Address          Local IP Address      Routing-Instance
-----
122.2.2.3               17.1.1.1             0
122.2.2.2               17.1.1.1             0
112.11.1.2              17.1.1.1             0

```

```

show unified-edge sgw gtp peer detail
user@host> show unified-edge sgw gtp peer detail
Gateway: SGW
Peer Detail:
-----
Remote IP Addr          : 136.6.6.2
Local IP Addr           : 17.1.1.1
Routing Instance        : 0
Interface Type          : GTP_INTF_S11
GTP Version              : 2
RCM Registration Done   : yes
Is Restart Counter Valid : yes
Restart Counter Value   : 1
Sent Restart Counter Value : 0

```

```
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
Downlink data notif delay Interval : 0
Is PATH Management Enabled (control) : yes
Is CSID Supported             : no
IS GTP-C using Short Seq Number : no
GTP-C Path State              : active
Data Path echo N3 Req         : 8
Data Path echo T3 Timer       : 15
Data Path Echo Interval       : 60
Is PATH Management Enabled (Data) : no
GTP-U Path State              : inactive
```

show unified-edge sgw gtp peer statistics

Syntax	<pre>show unified-edge sgw gtp peer statistics remote-address <i>remote-address</i> <detail> <fpc-slot <i>fpc-slot</i>> <gateway <i>gateway</i>> <local-address <i>local-address</i>> <pic-slot <i>pic-slot</i>> <routing-instance <i>routing-instance</i>></pre>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Display the GTP peer statistics for one or more Serving Gateways (S-GWs). If a gateway is not specified, then the statistics for all the S-GWs is displayed.
Options	<p>remote-address <i>remote-address</i>—Display the GTP peer statistics for the peer with the specified remote address.</p> <p>detail—(Optional) Display detailed statistics about GTP peers.</p> <p>fpc-slot <i>fpc-slot</i>—(Optional) Display the GTP peer statistics for the specified FPC slot number.</p> <p>gateway <i>gateway-name</i>—(Optional) Display the GTP peer statistics for the specified gateway.</p> <p>local-address <i>local-address</i>—(Optional) Display the GTP peer statistics for the local address of the specified peer on the S-GW.</p> <p>pic-slot <i>pic-slot</i>—(Optional) Display the GTP peer for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.</p> <p>routing-instance <i>routing-instance</i>—(Optional) Display the GTP peer statistics for the peer on the specified routing instance.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear unified-edge sgw gtp peer statistics on page 1197 • show unified-edge sgw gtp peer on page 1221 • show unified-edge sgw gtp statistics on page 1230
List of Sample Output	<p>show unified-edge sgw gtp peer statistics remote-address 136.6.6.2 on page 1226</p> <p>show unified-edge sgw gtp peer statistics remote-address 136.6.6.2 detail on page 1227</p>
Output Fields	See the output fields for the show unified-edge sgw gtp statistics command.

Sample Output

```

user@host> show unified-edge sgw gtp peer statistics remote-address 136.6.6.2
Gateway: SGW

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
GTP Unknown Version Received : 0
Packet Length Error Received : 0
Unknown Messages Received    : 0

GTP Version 2 Statistics:
-----
Protocol Error                : 0
Unsupported Messages Received : 0

-----

```

Message Type	Received	Transmitted
Total number of messages	25	25
Total number of bytes	325	1025
Redirect messages	0	0
S11 piggyback messages	0	0
S4 piggyback messages	0	0
S5 piggyback messages	0	0
Echo Request	0	25
Echo Response	25	0
Version Not Supported	0	0
Create session request	0	0
Create session response	0	0
Modify bearer request	0	0
Modify bearer response	0	0
Delete session request	0	0
Delete session response	0	0
Create bearer request	0	0
Create bearer response	0	0
Update bearer request	0	0
Update bearer response	0	0
Delete bearer request	0	0
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
Release Access Bearer request	0	0

Release Access Bearer response	0	0
Suspend Notification	0	0
Suspend Acknowledge	0	0
Resume Notification	0	0
Resume Acknowledge	0	0
Create Indirect Data Forward Tunnel Request	0	0
Create Indirect Data Forward Tunnel Response	0	0
Delete Indirect Data Forward Tunnel Request	0	0
Delete Indirect Data Forward Tunnel Response	0	0
Downlink Data Notification	0	0
Downlink Data Notification ack	0	0
Downlink Data Notification fail	0	0
Stop paging indication	0	0

```
show unified-edge sgw user@host> show unified-edge sgw gtp peer statistics remote-address 136.6.6.2 detail
gtp peer statistics Gateway: SGW
remote-address 136.6.6.2 detail
```

```
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
GTP Unknown Version Received  : 0
Packet Length Error Received  : 0
Unknown Messages Received     : 0
```

GTP Version 2 Statistics:

```
-----
Protocol Error                  : 0
Unsupported Messages Received  : 0
T3 Response Timer Expires      : 0
```

Message Type	Received	Transmitted

Total number of messages	26	26
Total number of bytes	338	1066
Redirect messages	0	0
S11 piggyback messages	0	0
S4 piggyback messages	0	0
S5 piggyback messages	0	0
Echo Request	0	26
Echo Response	26	0
Version Not Supported	0	0
Create session request	0	0
Create session response	0	0
Modify bearer request	0	0
Modify bearer response	0	0
Delete session request	0	0
Delete session response	0	0
Create bearer request	0	0
Create bearer response	0	0
Update bearer request	0	0
Update bearer response	0	0
Delete bearer request	0	0
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
Release Access Bearer request	0	0
Release Access Bearer response	0	0
Suspend Notification	0	0
Suspend Acknowledge	0	0
Resume Notification	0	0
Resume Acknowledge	0	0
Create Indirect Data Forward Tunnel Request	0	0
Create Indirect Data Forward Tunnel Response	0	0
Delete Indirect Data Forward Tunnel Request	0	0
Delete Indirect Data Forward Tunnel Response	0	0
Downlink Data Notification	0	0
Downlink Data Notification ack	0	0
Downlink Data Notification fail	0	0
Stop paging indication	0	0

Cause Code	Received	Transmitted

Request accepted	0	0
Request accepted partially	0	0
New PDN type due to network preference	0	0
New PDN type due to single address bearer only	0	0
Local Detach	0	0
Complete Detach	0	0
RAT changed from 3GPP to Non 3GPP	0	0
ISR Deactivated	0	0
Error Indication from RNC Enodeb	0	0
Context Not Found	0	0
Invalid Message Format	0	0
Version not supported by next peer	0	0
Invalid length	0	0
Service not supported	0	0
Mandatory IE incorrect	0	0
Mandatory IE missing	0	0
Optional IE incorrect	0	0
System failure	0	0
No resources available	0	0
Semantic error in the TFT operation	0	0
Syntactic error in the TFT operation	0	0
Semantic errors in packet filter(s)	0	0
Syntactic errors in packet filter(s)	0	0
Missing or unknown APN	0	0
Unexpected repeated IE	0	0
GRE key not found	0	0
Reallocation failure	0	0
Denied in RAT	0	0
Preferred PDN type not supported	0	0
All dynamic addresses are occupied	0	0

UE context without TFT already activated	0	0
Protocol type not supported	0	0
UE not responding	0	0
UE refuses	0	0
Service denied	0	0
Unable to page UE	0	0
No memory available	0	0
User authentication failed	0	0
APN access denied - no subscription	0	0
Request rejected	0	0
P-TMSI Signature Mismatch	0	0
IMSI Not Known	0	0
Semantic Error in the TAD Operation	0	0
Syntactic Error in the TAD Operation	0	0
Reserved Message Value Received	0	0
Rmt Peer Not Responding	0	0
Collision with Network Initiated Request	0	0
Unable to Page UE due to Suspension	0	0
Conditional IE Missing	0	0
APN Restriction Type Incompatible	0	0
Invalid Total len	0	0
Data Forwarding Not Supported	0	0
Invalid Reply from Rmt Peer	0	0
Invalid Peer	0	0
Unknown	0	0

show unified-edge sgw gtp statistics

Syntax	<pre>show unified-edge sgw gtp statistics <detail> <fpc-slot fpc-slot> <gateway gateway> <pic-slot pic-slot></pre>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Display the global GTP statistics for one or more Serving Gateways (S-GWs). If a gateway is not specified, then statistics for all S-GWs are displayed.
Options	<p>none—Display the GTP statistics in brief.</p> <p>detail—(Optional) Display the GTP statistics with the GTP cause statistics included.</p> <p>fpc-slot fpc-slot—(Optional) Display the GTP statistics for the specified FPC slot number.</p> <p>gateway gateway-name—(Optional) Display the GTP statistics for the specified gateway.</p> <p>pic-slot pic-slot—(Optional) Display the GTP statistics for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear unified-edge sgw gtp statistics on page 1198 show unified-edge sgw gtp peer statistics on page 1225
List of Sample Output	<p>show unified-edge sgw gtp statistics on page 1232</p> <p>show unified-edge sgw gtp statistics detail on page 1233</p>
Output Fields	Table 99 on page 1230 lists the output fields for the show unified-edge sgw gtp statistics command. Output fields are listed in the approximate order in which they appear.

Table 99: show unified-edge sgw gtp statistics Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the S-GW.	All levels
Global Packet Statistics		
Received Packets Dropped	Total number of packets received by the S-GW that were dropped.	All levels
Packet Allocation Fail	Number of times that packet allocation failed.	All levels
Packet Send Fail	Number of times that packet sending failed.	All levels
IP Version Error Received	Number of packets with an unsupported IP version.	All levels

Table 99: show unified-edge sgw gtp statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
IP Protocol Error Received	Number of non-UDP IP packets received.	All levels
GTP Port Error Received	Number of packets received on a unknown GTP port number.	All levels
GTP Unknown Version Received	Number of GTP packets with an incorrect GTP version.	All levels
Packet Length Error Received	Number of GTP packets with incorrect length in the IP or UDP header.	All levels
Unknown Messages Received	Number of GTP messages received that are not recognized by the S-GW.	All levels
GTP Version 2 Statistics		
Protocol Error	Number of messages received that had a protocol error. This counter is incremented if a message with an invalid or unknown GTP message type is received.	All levels
Unsupported Messages Received	Number of messages received that had a protocol error. This counter is incremented if a message with an invalid or unknown GTP message type is received.	All levels
T3 Response Timer Expires	Number of messages for which the T3 response timer elapsed.	All levels
Message Type	Type of the GTP message; for example, S11 piggyback messages or Create session response .	All levels
Received	Number of GTP messages received corresponding to the message type.	All levels
Transmitted	Number of GTP messages transmitted corresponding to the message type.	All levels
Cause Code	GTP cause codes; for example, Request accepted or Missing or unknown APN .	detail
Received	Number of GTP messages received corresponding to the GTP cause code.	detail
Transmitted	Number of GTP messages transmitted corresponding to the GTP cause code.	detail
Error Indication Statistics		
Version	GTP version (GTP version 0 and GTP version 1) for which the error indication statistics are displayed.	All levels
Received	Number of error indication messages received, corresponding to the GTP version.	All levels

Table 99: show unified-edge sgw gtp statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
Transmitted	Number of error indication messages transmitted, corresponding to the GTP version.	All levels

Sample Output

```
show unified-edge sgw gtp statistics
user@host> show unified-edge sgw gtp statistics
Gateway: SGW
```

```
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
GTP Unknown Version Received : 0
Packet Length Error Received : 0
Unknown Messages Received    : 0
```

GTP Version 2 Statistics:

```
-----
Protocol Error                : 0
Unsupported Messages Received : 0
T3 Response Timer Expires    : 0
```

Message Type	Received	Transmitted
-----	-----	-----
Total number of messages	923	924
Total number of bytes	9191	13225
Redirect messages	0	0
S11 piggyback messages	0	0
S4 piggyback messages	0	0
S5 piggyback messages	0	0
Echo Request	907	0
Echo Response	0	907
Version Not Supported	0	0
Create session request	3	3
Create session response	3	3
Modify bearer request	3	0
Modify bearer response	0	3
Delete session request	6	5
Delete session response	1	3
Create bearer request	0	0
Create bearer response	0	0
Update bearer request	0	0
Update bearer response	0	0
Delete bearer request	0	0
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
Release Access Bearer request	0	0
Release Access Bearer response	0	0
Create Indirect Data Forward Tunnel Request	0	0
Create Indirect Data Forward Tunnel Response	0	0
Delete Indirect Data Forward Tunnel Request	0	0
Delete Indirect Data Forward Tunnel Response	0	0
Downlink Data Notification	0	0
Downlink Data Notification ack	0	0
Downlink Data Notification fail	0	0
Stop paging indication	0	0

Error Indication Statistics:

Version	Received	Transmitted

GTPv0	0	0
GTPv1	0	0

```
show unified-edge sgw gtp statistics detail
user@host> show unified-edge sgw gtp statistics detail
Gateway: SGW
```

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
GTP Unknown Version Received	: 0
Packet Length Error Received	: 0
Unknown Messages Received	: 0

GTP Version 2 Statistics:

Protocol Error	: 0
Unsupported Messages Received	: 0
T3 Response Timer Expires	: 0

Message Type	Received	Transmitted

Total number of messages	925	926
Total number of bytes	9209	13251
Redirect messages	0	0
S11 piggyback messages	0	0
S4 piggyback messages	0	0
S5 piggyback messages	0	0
Echo Request	909	0
Echo Response	0	909
Version Not Supported	0	0
Create session request	3	3
Create session response	3	3
Modify bearer request	3	0
Modify bearer response	0	3

Delete session request	6	5
Delete session response	1	3
Create bearer request	0	0
Create bearer response	0	0
Update bearer request	0	0
Update bearer response	0	0
Delete bearer request	0	0
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
Release Access Bearer request	0	0
Release Access Bearer response	0	0
Create Indirect Data Forward Tunnel Request	0	0
Create Indirect Data Forward Tunnel Response	0	0
Delete Indirect Data Forward Tunnel Request	0	0
Delete Indirect Data Forward Tunnel Response	0	0
Downlink Data Notification	0	0
Downlink Data Notification ack	0	0
Downlink Data Notification fail	0	0
Stop paging indication	0	0

Cause Code	Received	Transmitted

Request accepted	4	9
Request accepted partially	0	0
New PDN type due to network preference	0	0
New PDN type due to single address bearer only	0	0
Context Not Found	0	0
Invalid Message Format	0	0
Version not supported by next peer	0	0
Invalid length	0	0
Service not supported	0	0
Mandatory IE incorrect	0	0
Mandatory IE missing	0	0
Optional IE incorrect	0	0
System failure	0	0
No resources available	0	0
Semantic error in the TFT operation	0	0
Syntactic error in the TFT operation	0	0
Semantic errors in packet filter(s)	0	0
Syntactic errors in packet filter(s)	0	0
Missing or unknown APN	0	0
Unexpected repeated IE	0	0
GRE key not found	0	0
Reallocation failure	0	0
Denied in RAT	0	0
Preferred PDN type not supported	0	0
All dynamic addresses are occupied	0	0
UE context without TFT already activated	0	0
Protocol type not supported	0	0
UE not responding	0	0
UE refuses	0	0

Service denied	0	0
Unable to page UE	0	0
No memory available	0	0
User authentication failed	0	0
APN access denied - no subscription	0	0
Request rejected	0	0
P-TMSI Signature Mismatch	0	0
IMSI Not Known	0	0
Conditional IE Missing	0	0
APN Restriction Type Incompatible	0	0
Unknown	0	0

Error Indication Statistics:

Version	Received	Transmitted

GTPv0	0	0
GTPv1	0	0

CHAPTER 36

Service Applications Operational Commands

show services flows (Aggregated Multiservices)

Syntax **show services flows**
 <brief | extensive | terse>
 <application-protocol *protocol*>
 <count>
 <destination-port *destination-port*>
 <destination-prefix *destination-prefix*>
 <interface *interface-name*>
 <limit *number*>
 <protocol *protocol*>
 <service-set *service-set*>
 <source-port *source-port*>
 <source-prefix *source-prefix*>

Release Information Command introduced in Junos OS Release 9.5.
 Support for aggregated multiservices (AMS) introduced in Junos OS Mobility Release 11.2W.

Description Display the flow session table entries for the active members of the AMS interface for services applications.

Options **none**—Display standard information about all flows.

brief | extensive | terse—(Optional) Display the specified level of output.

application-protocol—(Optional) Display information about one of the following application protocols:

- **ftp**—File Transfer Protocol
- **icmp**—Internet Control Message Protocol
- **pptp**—Point-to-Point Tunneling Protocol
- **rtsp**—Real-Time Streaming Protocol
- **sqlnet**—SQL *Net
- **tcp**—Transmission Control Protocol
- **traceroute**—Traceroute
- **tftp**—Trivial File Transfer Protocol
- **udp**—User Datagram Protocol

count—(Optional) Display a count of the total number of flows of the service sets in each member interface of the AMS.

destination-port *destination-port*—(Optional) Display information for the specified destination port. The range is from 0 through 65,535.

destination-prefix *destination-prefix*—(Optional) Display information for the specified destination prefix.

interface *interface-name*—(Optional) Display information about the specified interface. The **interface-name** is in the format **ms-fpc/pic/port**.

limit *number*—(Optional) Restrict the maximum number of entries displayed to the specified limit.

protocol *protocol*—(Optional) Display information about one of the following IP types:

- **number**—Numeric protocol value from 0 through 255
- **ah**—IPsec Authentication Header protocol
- **egp**—Exterior gateway protocol
- **esp**—IPsec Encapsulating Security Payload protocol
- **gre**—Generic routing encapsulation protocol
- **icmp**—Internet Control Message Protocol
- **icmp6**—Internet Control Message Protocol version 6
- **igmp**—Internet Group Management Protocol
- **ipip**—IP-over-IP encapsulation protocol
- **ospf**—Open Shortest Path First protocol
- **pim**—Protocol Independent Multicast protocol
- **rsvp**—Resource Reservation Protocol
- **sctp**—Stream Control Transmission Protocol
- **tcp**—Transmission Control Protocol
- **udp**—User Datagram Protocol

service-set *service-set*—(Optional) Display information for the specified service set.

source-port *source-port*—(Optional) Display information for the specified source port. The range is from 0 through 65,535.

source-prefix *source-prefix*—(Optional) Display information for the specified source prefix.

Required Privilege Level	view
List of Sample Output	show services flows interface ams0 on page 1240 show services flows count interface ams0 on page 1241
Output Fields	Table 100 on page 1240 lists the output fields for the show services flows (aggregated multiservices) command. Output fields are listed in the approximate order in which they appear.

Table 100: show services flows Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the aggregated multiservices member interface (mams-) and the aggregated multiservices interface (ams) to which it belongs.	All levels
Service set	Name of a service set. Individual empty service sets are not displayed. If no service set has any flows, a flow table header is displayed for each service set.	All levels
Flow Count	Number of flows in a session.	count only
Flow or Flow Prot	Protocol used for this flow.	All levels
Source	Source prefix of the flow in the format <i>source-prefix:port</i> . For ICMP flows, port information is not displayed.	All levels
Dest	Destination prefix of the flow. For ICMP flows, port information is not displayed.	All levels
State	Status of the flow: <ul style="list-style-type: none"> • Drop—Drop all packets in the flow without response. • Forward—Forward the packet in the flow without looking at it. • Reject—Drop all packets in the flow with response. • Watch—Inspect packets in the flow. 	All levels
Dir	Direction of the flow: input (I) or output (O).	All levels
Frm count	Number of frames in the flow.	All levels
Byte count	Number of bytes in the flow.	extensive
Flow role	Flow role.	extensive
Timeout	Timeout value.	extensive
Flow path	Flow path: symmetric or asymmetric.	extensive

Sample Output

```

show services flows user@host> show services flows interface ams0
interface ams0      Interface: mams-1/0/0 (ams0), Service set: napt_set
Flow               State   Dir   Frm count
UDP                30.30.30.2:63 -> 40.40.40.2:63 Forward I      83185
UDP                40.40.40.2:63 -> 30.30.30.160:6000 Forward O        0

```

```
show services flows count interface ams0
```

Interface	Service set	Flow count
mams-1/0/0	napt_set	38
mams-1/0/0	ssl	0
mams-1/1/0	napt_set	36
mams-1/1/0	ssl	0
mams-5/0/0	napt_set	18
mams-5/0/0	ssl	0
mams-5/1/0	napt_set	34
mams-5/1/0	ssl	0

show services nat mappings app

Syntax `show services nat mappings app`
`<pool-name>`

Release Information Command introduced in Junos OS Mobility Release 11.2W.

Description Display the Network Address Translation (NAT) mappings for paired IP address pooling (or address pooling paired [APP]) for the NAT pools on the multiservices interface.

Options *pool-name*—(Optional) Display the NAT mappings for the NAT pool specified. (The NAT pools are configured at the `[edit services nat]` hierarchy level.)

Required Privilege Level view

Related Documentation

- [show services nat mappings eim on page 1244](#)
- [show services nat mappings summary on page 1246](#)

List of Sample Output [show services nat mappings app on page 1243](#)

Output Fields [Table 101 on page 1242](#) lists the output fields for the `show services nat mappings app` command. Output fields are listed in the approximate order in which they appear.

Table 101: show services nat mappings app Output Fields

Field Name	Field Description
Interface	Name of the multiservices interface (ms- or mams-).
Service set	Name of the service set for which the NAT mappings are displayed.
NAT pool	Name of the NAT pool.
Internal Address	Internal IP address that is being mapped.
External Address	External IP address to which the internal address is mapped.
Number of sessions	Number of sessions for which the NAT mapping has been done.
State	NAT mapping state. The following states are possible: <ul style="list-style-type: none"> • ACTIVE—Indicates that the entry is active and in use. • TIMEOUT—Indicates that the entry is not in use and will be deleted after the mapping-timeout, configured at the <code>[edit services nat pool <i>pool-name</i>]</code> hierarchy level, lapses.

Sample Output

```
show services nat mappings app
user@host> show services nat mappings app
Interface: ms-1/0/0, Service set: ss

NAT pool: p1
Internal Address  External Address  Number of sessions  State
10.10.10.3        30.30.30.3        1                    ACTIVE
10.10.10.2        30.30.30.2        2                    ACTIVE
```

show services nat mappings eim

Syntax	show services nat mappings eim <pool-name>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Display the Network Address Translation (NAT) mappings for Endpoint Independent Mapping (EIM) for the NAT pools on the multiservices interface.
Options	pool-name —(Optional) Display the NAT mappings for the NAT pool specified. (The NAT pools are configured at the [edit services nat] hierarchy level.)
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show services nat mappings app on page 1242 • show services nat mappings summary on page 1246
List of Sample Output	show services nat mappings eim on page 1245
Output Fields	Table 102 on page 1244 lists the output fields for the show services nat mappings eim command. Output fields are listed in the approximate order in which they appear.

Table 102: show services nat mappings eim Output Fields

Field Name	Field Description
Interface	Name of the multiservices interface (ms- or mams-).
Service set	Name of the service set for which the NAT mappings are displayed.
NAT pool	Name of the NAT pool.
Internal Address: Port	Internal IP address and the port that are being mapped.
External Address: Port	External IP address and the port to which the internal address and port are mapped.
Number of sessions	Number of sessions for which the NAT mapping has been done.
State	<p>NAT mapping state. The following states are possible:</p> <ul style="list-style-type: none"> • ACTIVE—Indicates that the entry is active and in use. • TIMEOUT—Indicates that the entry is not in use and will be deleted after the mapping-timeout, configured at the [edit services nat pool pool-name] hierarchy level, lapses.

Sample Output

```
show services nat mappings eim user@host> show services nat mappings eim
mappings eim                  Interface: ms-1/0/0, Service set: ss

NAT pool: p1
Internal Address  External Address  Number of sessions  State
10.10.10.3       30.30.30.3       1                   ACTIVE
10.10.10.2       30.30.30.2       2                   ACTIVE
```

show services nat mappings summary

Syntax	show services nat mappings summary
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Display the summary information about the Network Address Translation (NAT) mappings for the active multiservices interfaces.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show services nat mappings app on page 1242• show services nat mappings eim on page 1244
List of Sample Output	show services nat mappings summary on page 1246
Output Fields	Table 103 on page 1246 lists the output fields for the show services nat mappings summary command. Output fields are listed in the approximate order in which they appear.

Table 103: show services nat mappings summary Output Fields

Field Name	Field Description
Interface	Name of the multiservices interface (ms- or mams-).
Total number of address mappings	Total number of address pooling paired (APP) mappings.
Total number of endpoint independent port mappings	Total number of endpoint-independent port mappings.

Sample Output

```
show services nat mappings summary  user@host> show services nat mappings summary
                                     Interface Name:                               ms-1/0/0
                                     Total number of address mappings:                1
                                     Total number of endpoint independent port mappings: 2
```

show services nat pool (Aggregated Multiservices)

Syntax	show services nat pool <brief detail> <pool-name>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Display information about the Network Address Translation (NAT) pools and their current split among the active aggregated multiservices (AMS) member interfaces. In AMS NAT, the pool might be split among the active members based on the NAT type configured.
Options	<p>none—Display standard information about all the NAT pools for the ams interface.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>pool-name—(Optional) Display information about the specified NAT pool.</p>
Required Privilege Level	view
List of Sample Output	show services nat pool brief (Aggregated Multiservices) on page 1248 show services nat pool detail (Aggregated Multiservices) on page 1248 show services nat pool dynamic_pool detail on page 1249
Output Fields	Table 104 on page 1247 lists the output fields for the show services nat pool (aggregated multiservices) command. Output fields are listed in the approximate order in which they appear.

Table 104: show services nat pool Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the aggregated multiservices member interface (mams-) and the aggregated multiservices interface (ams) to which it belongs.	All levels
Service set	Name of the service set for the interface. Individual empty service sets are not displayed, but if none of the service sets has any flows, a flow table header is printed for each service set.	All levels
NAT pool	Name of the NAT pool for the interface.	All levels
Type or Translation type	Address translation type: basic-nat-pt , basic-nat44 , dnat-44 , dynamic-nat44 , NAPT-44 , or napt-pt .	All levels
Address or Address range	IPv4 address range of the pool.	All levels
Port or Port range	Port range of the pool. This is applicable only for dynamic NAT pools and is not displayed for static NAT pools.	All levels

Table 104: show services nat pool Output Fields (*continued*)

Field Name	Field Description	Level of Output
Ports used or Ports in use	Number of ports allocated in this pool with this name. This is applicable only for dynamic NAT pools and is not displayed for static NAT pools.	All levels
Out of port errors	Number of port allocation errors. This is applicable only for dynamic NAT pools and is not displayed for static NAT pools.	detail
Max ports used	Maximum number of ports used. This is applicable only for dynamic NAT pools and is not displayed for static NAT pools.	detail
Addresses in use	Number of addresses in use for dynamic source address NAT pools.	detail

Sample Output

```

user@host> show services nat pool brief
show services nat pool brief (Aggregated Multiservices)
Interface: mams-1/0/0 (ams0), Service set: napt_set
NAT pool      Type      Address                               Port      Ports used
napt_pool     NAPT-44   30.30.30.160-30.30.30.163           6000-8000 1
              30.30.30.176-30.30.30.176
Interface: mams-1/1/0 (ams0), Service set: napt_set
NAT pool      Type      Address                               Port      Ports used
napt_pool     NAPT-44   30.30.30.164-30.30.30.167           6000-8000 0
Interface: mams-5/0/0 (ams0), Service set: napt_set
NAT pool      Type      Address                               Port      Ports used
napt_pool     NAPT-44   30.30.30.168-30.30.30.171           6000-8000 0
Interface: mams-5/1/0 (ams0), Service set: napt_set
NAT pool      Type      Address                               Port      Ports used
napt_pool     NAPT-44   30.30.30.172-30.30.30.175           6000-8000 0

user@host> show services nat pool detail
show services nat pool detail (Aggregated Multiservices)
Interface: mams-1/0/0 (ams0), Service set: napt_set
NAT pool: napt_pool, Translation type: NAPT-44
Address range: 30.30.30.160-30.30.30.163
Address range: 30.30.30.176-30.30.30.176
Port range: 6000-8000, Ports in use: 19, Out of port errors: 0, Max ports
used: 19

Interface: mams-1/1/0 (ams0), Service set: napt_set
NAT pool: napt_pool, Translation type: NAPT-44
Address range: 30.30.30.164-30.30.30.167
Port range: 6000-8000, Ports in use: 18, Out of port errors: 0, Max ports
used: 18

Interface: mams-5/0/0 (ams0), Service set: napt_set
NAT pool: napt_pool, Translation type: NAPT-44
Address range: 30.30.30.168-30.30.30.171
Port range: 6000-8000, Ports in use: 9, Out of port errors: 0, Max ports used:
9

Interface: mams-5/1/0 (ams0), Service set: napt_set
NAT pool: napt_pool, Translation type: NAPT-44
Address range: 30.30.30.172-30.30.30.175
Port range: 6000-8000, Ports in use: 17, Out of port errors: 0, Max ports

```

used: 17

**show services nat pool
dynamic_pool detail**

user@host> show services nat pool dynamic_pool detail

Interface: mams-1/0/0 (ams0), Service set: napt_set

NAT pool: napt_pool, Translation type: NAPT-44

Address range: 30.30.30.160-30.30.30.163

Address range: 30.30.30.176-30.30.30.176

Port range: 6000-8000, Ports in use: 19, Out of port errors: 0, Max ports
used: 19

Interface: mams-1/1/0 (ams0), Service set: napt_set

NAT pool: napt_pool, Translation type: NAPT-44

Address range: 30.30.30.164-30.30.30.167

Port range: 6000-8000, Ports in use: 18, Out of port errors: 0, Max ports
used: 18

Interface: mams-5/0/0 (ams0), Service set: napt_set

NAT pool: napt_pool, Translation type: NAPT-44

Address range: 30.30.30.168-30.30.30.171

Port range: 6000-8000, Ports in use: 9, Out of port errors: 0, Max ports used:
9

Interface: mams-5/1/0 (ams0), Service set: napt_set

NAT pool: napt_pool, Translation type: NAPT-44

Address range: 30.30.30.172-30.30.30.175

Port range: 6000-8000, Ports in use: 17, Out of port errors: 0, Max ports
used: 17

show services nat statistics

Syntax	show services nat statistics <interface <i>interface</i>>
Release Information	Command introduced in Junos OS Mobility Release 11.2W.
Description	Display the NAT statistics for the multiservices interfaces present on the broadband gateway.
Options	interface <i>interface</i> —Name of the extension provider interface.
Required Privilege Level	view
List of Sample Output	show services nat statistics on page 1255
Output Fields	Table 105 on page 1250 lists the output fields for the show services nat statistics command. Output fields are listed in the approximate order in which they appear. Some of these fields are used internally by Juniper's engineers for troubleshooting.

Table 105: show services nat statistics Output Fields

Field Name	Field Description
Interface	Name of the multiservices interface.
Session Statistics	
Total Session Interest events	Total number of Session Interest events.
Total Session Create events	Total number of Session Create events.
Total Session Destroy events	Total number of Session Destroy events.
Total Session Pub Req events	Total number of Session Pub Req events.
Total Session Accepts	Total number of sessions accepted.
Total Session Discards	Total number of sessions discarded.
Total Session Ignores	Total number of sessions ignored.
Session interest thru pub event	Session interest through pub event.

Table 105: show services nat statistics Output Fields (*continued*)

Field Name	Field Description
ALG Session interest	Application-level gateway (ALG) session interest.
ALG Session Create	ALG Session Create
Packet Dst in NAT route	Sessions discarded due to packet destination in the NAT route.
Session Ext Alloc Failures	Session extension allocation failures.
Session Ext Set Failures	Session extension set failures.
Session Created for EIF	Number of sessions created for Endpoint Independent Filtering (EIF).
Session Created for EIM	Number of sessions created for Endpoint Independent Mapping (EIM).
NAT rule lookup failures	Number of NAT rule lookup failures.
NAT Allocation Statistics	
NAT allocation Successes	Number of successful NAT map allocations.
NAT allocation Failures	Number of NAT map allocation failures.
NAT Free Successes	NAT free successes.
NAT Free Failures	NAT free failures.
NAT EIM mapping reused	Number of NAT EIM mappings reused.
NAT EIM mapping allocation failures	Number of NAT EIM mapping allocation failures.
NAT EIM mapping Duplicate entry	Number of duplicate NAT EIM mappings.
NAT EIM mapping create failed	Number of failed NAT EIM mappings.
NAT EIM mapping Created	Number of NAT EIM mappings created.

Table 105: show services nat statistics Output Fields (*continued*)

Field Name	Field Description
NAT EIF mapping Free	Number of free NAT EIF mappings.
NAT EIM mapping Free	Number of free NAT EIM mappings.
NAT EIM waiting for init	Number of NAT EIM mappings waiting for initialization.
NAT EIM waiting for init failed	Number of NAT EIM mappings that failed initialization.
NAT EIM lookup and hold success	Number of successful NAT EIM lookups and holds.
NAT EIM lookup entry in timeout	NAT EIM lookup entry in timeout.
NAT EIM lookup timer cleared for timeout entry	NAT EIM lookup timer cleared for timeout entry.
NAT EIM lookup timeout entry without timer	NAT EIM lookup timeout entry without timer.
NAT EIM release without entry	NAT EIM release without entry.
NAT EIM release entry in timeout	NAT EIM release entry in timeout.
NAT EIM release race	NAT EIM release race.
NAT EIM release set entry for timeout	NAT EIM release set entry for timeout.
NAT EIM timer entry refreshed	NAT EIM timer entry refreshed.
NAT EIM timer invalid timer started	NAT EIM timer invalid timer started.
NAT EIM timer entry freed	NAT EIM timer entry freed.

Packet Statistics

Table 105: show services nat statistics Output Fields (*continued*)

Field Name	Field Description
Total Packets Processed	Total number of packets processed.
Total Packets Forwarded	Total number of packets forwarded.
Total Packets Discarded	Total number of packets discarded.
Total Packets Translated	Total number of packets translated.
Total Packets Restored	Total number of packets restored.
Translation Statistics	
Src IPv4 Translations	Number of source IPv4 translations.
Src IPv4 Restorations	Number of source IPv4 restorations.
Dst IPv4 Translations	Number of destination IPv4 translations.
Dst IPv4 Restorations	Number of destination IPv4 restorations.
Src Port Translations	Number of source port translations.
Src Port Restorations	Number of source port restorations.
Dst Port Translations	Number of destination port translations.
Dst Port Restorations	Number of destination port restorations.
ICMP ID Translations	Number of Internet Control Message Protocol (ICMP) translations.
ICMP ID Restorations	Number of ICMP restorations.
ICMP Error Translations	Number of ICMP error packets after translations.

Table 105: show services nat statistics Output Fields (*continued*)

Field Name	Field Description
TCP Port Translations	Number of TCP port translations.
TCP Port Restorations	Number of TCP port restorations.
UDP Port Translations	Number of UDP port translations.
UDP Port Restorations	Number of UDP port restorations.
GRE Call ID Translations	Number of generic routing encapsulation (GRE) call ID translations.
GRE Call ID Restorations	Number of GRE call ID restorations.
SRC IP restored in ICMP Error	Source IP restored in ICMP Error.
DST IP restored in ICMP Error	DST IP restored in ICMP Error.
SRC IP translated in ICMP Error	SRC IP translated in ICMP Error.
DST IP translated in ICMP Error	Destination IP translated in ICMP Error.
New SRC IP translated in ICMP Error	New source IP translated in ICMP Error.
Inner SRC IP restored in ICMP Error	Inner source IP restored in ICMP Error.
Inner SRC port restored in ICMP Error	Inner source port restored in ICMP Error.
Inner DST IP restored in ICMP Error	Inner destination IP restored in ICMP Error.
Inner SRC IP Translated in ICMP Error	Inner source IP translated in ICMP Error.

Table 105: show services nat statistics Output Fields (*continued*)

Field Name	Field Description
Inner SRC port Translated in ICMP Error	Inner source port translated in ICMP Error.
Inner DST IP Translated in ICMP Error	Inner destination IP translated in ICMP Error.
Misc Errors	
NAT error - no policy	Number of NAT errors of the no policy type.
NAT error - xlate free called with null ext	Number of NAT errors of the xlate free called with null ext type.
NAT error - ext free failed	Number of NAT errors of the ext free failed type.
NAT error - policy add failed	Number of NAT errors of the policy add failed type.
NAT error - policy delete failed	Number of NAT errors of the policy delete failed type.

Sample Output

```

show services nat statistics user@host> show services nat statistics
statistics                 Interface: ms-0/0/0

Session statistics
  Total Session Interest events      :12315
  Total Session Create events        :2
  Total Session Destroy events       :12315
  Total Session Pub Req events       :0
  Total Session Accepts               :12315
  Total Session Discards              :0
  Total Session Ignores               :0
  Session interest thru pub event     :0
  ALG Session interest                :0
  ALG Session Create                 :0
  Packet Dst in NAT route             :0
  Session Ext Alloc Failures          :0
  Session Ext Set Failures            :0
  Session Created for EIF              :1
  Session Created for EIM             :12314
  NAT rule lookup failures            :0

NAT Allocation statistics
  NAT allocation Successes            :12314
  NAT allocation Failures             :0
  NAT Free Successes                  :0

```

NAT Free Failures	:0
NAT EIM mapping reused	:12312
NAT EIM mapping allocation failures	:0
NAT EIM mapping Duplicate entry	:0
NAT EIM mapping create failed	:0
NAT EIM mapping Created	:2
NAT EIF mapping Free	:1
NAT EIM mapping Free	:12314
NAT EIM waiting for init	:0
NAT EIM waiting for init failed	:0
NAT EIM lookup and hold success	:12313
NAT EIM lookup entry in timeout	:0
NAT EIM lookup timer cleared for timeout entry	:0
NAT EIM lookup timeout entry without timer	:0
NAT EIM release without entry	:0
NAT EIM release entry in timeout	:0
NAT EIM release race	:0
NAT EIM release set entry for timeout	:2
NAT EIM timer entry refreshed	:0
NAT EIM timer invalid timer started	:2
NAT EIM timer entry freed	:2
Packet statistics	
Total Packets Processed	:2715735062
Total Packets Forwarded	:2715735062
Total Packets Discarded	:0
Total Packets Translated	:1818000836
Total Packets Restored	:897734226
Translation statistics	
Src IPv4 Translations	:400996
Src IPv4 Restorations	:897734226
Dst IPv4 Translations	:1817599840
Dst IPv4 Restorations	:0
Src Port Translations	:400996
Src Port Restorations	:897734226
Dst Port Translations	:1817599840
Dst Port Restorations	:0
ICMP ID Translations	:0
ICMP ID Restorations	:0
ICMP Error Translations	:0
TCP Port Translations	:0
TCP Port Restorations	:0
UDP Port Translations	:1818000836
UDP Port Restorations	:897734226
GRE CallID Translations	:0
GRE CallID Restorations	:0
SRC IP restored in ICMP Error	:0
DST IP restored in ICMP Error	:0
SRC IP translated in ICMP Error	:0
DST IP translated in ICMP Error	:0
New SRC IP translated in ICMP Error	:0
Inner SRC IP restored in ICMP Error	:0
Inner SRC port restored in ICMP Error	:0
Inner DST IP restored in ICMP Error	:0
Inner SRC IP Translated in ICMP Error	:0
Inner SRC port Translated in ICMP Error	:0
Inner DST IP Translated in ICMP Error	:0
Misc Errors	
NAT error - no policy	:0

```

NAT error - xlate free called with null ext      :0
NAT error - ext free failed                      :0
NAT error - policy add failed                   :0
NAT error - policy delete failed                :0

Interface: ms-1/1/0

Session statistics
  Total Session Interest events                  :6
  Total Session Create events                   :6
  Total Session Destroy events                  :7
  Total Session Pub Req events                  :0
  Total Session Accepts                        :6
  Total Session Discards                      :0
  Total Session Ignores                      :0
  Session interest thru pub event              :0
  ALG Session interest                        :0
  ALG Session Create                          :0
  Packet Dst in NAT route                     :0
  Session Ext Alloc Failures                   :0
  Session Ext Set Failures                     :0
  Session Created for EIF                      :0
  Session Created for EIM                     :6
  NAT rule lookup failures                     :0

NAT Allocation statistics
  NAT allocation Successes                     :6
  NAT allocation Failures                      :0
  NAT Free Successes                          :0
  NAT Free Failures                           :0
  NAT EIM mapping reused                      :3
  NAT EIM mapping allocation failures          :0
  NAT EIM mapping Duplicate entry             :0
  NAT EIM mapping create failed                :0
  NAT EIM mapping Created                     :3
  NAT EIF mapping Free                        :0
  NAT EIM mapping Free                        :7
  NAT EIM waiting for init                     :0
  NAT EIM waiting for init failed              :0
  NAT EIM lookup and hold success              :2
  NAT EIM lookup entry in timeout              :1
  NAT EIM lookup timer cleared for timeout entry :1
  NAT EIM lookup timeout entry without timer   :0
  NAT EIM release without entry                :0
  NAT EIM release entry in timeout             :0
  NAT EIM release race                        :0
  NAT EIM release set entry for timeout        :5
  NAT EIM timer entry refreshed                :0
  NAT EIM timer invalid timer started          :4
  NAT EIM timer entry freed                    :4

Packet statistics
  Total Packets Processed                      :2733886586
  Total Packets Forwarded                      :2733886586
  Total Packets Discarded                      :0
  Total Packets Translated                     :1836152360
  Total Packets Restored                       :897734226

Translation statistics
  Src IPv4 Translations                       :1836152360
  Src IPv4 Restorations                       :0

```

Dst IPv4	Translations	:0
Dst IPv4	Restorations	:897734226
Src Port	Translations	:1836152360
Src Port	Restorations	:0
Dst Port	Translations	:0
Dst Port	Restorations	:897734226
ICMP ID	Translations	:0
ICMP ID	Restorations	:0
ICMP Error	Translations	:0
TCP Port	Translations	:0
TCP Port	Restorations	:0
UDP Port	Translations	:1836152360
UDP Port	Restorations	:897734226
GRE CallID	Translations	:0
GRE CallID	Restorations	:0
SRC IP	restored in ICMP Error	:0
DST IP	restored in ICMP Error	:0
SRC IP	translated in ICMP Error	:0
DST IP	translated in ICMP Error	:0
New SRC IP	translated in ICMP Error	:0
Inner SRC IP	restored in ICMP Error	:0
Inner SRC port	restored in ICMP Error	:0
Inner DST IP	restored in ICMP Error	:0
Inner SRC IP	Translated in ICMP Error	:0
Inner SRC port	Translated in ICMP Error	:0
Inner DST IP	Translated in ICMP Error	:0
Misc Errors		
NAT error - no policy		:0
NAT error - xlate free called with null ext		:0
NAT error - ext free failed		:0
NAT error - policy add failed		:0
NAT error - policy delete failed		:0

show services service-sets summary

Syntax	show services service-sets summary <interface <i>interface</i>>
Release Information	Command introduced before Junos OS Release 7.4. Display of the CPU usage in the output introduced in Junos OS Mobility Release 11.2W.
Description	Display the summary information about the service sets for multiservices (MS) interfaces.
Options	interface <i>interface</i> —Name of the adaptive services interface (ms-).
Required Privilege Level	view
List of Sample Output	show services service-sets summary on page 1259
Output Fields	Table 106 on page 1259 lists the output fields for the show services service-sets summary command. Output fields are listed in the approximate order in which they appear.

Table 106: show services service-sets summary Output Fields

Field Name	Field Description
Interface	Name of the multiservices member interface (ms-).
Service sets configured	Total number of service sets configured on the interface.
Bytes used	Total number of bytes used by stateful services for runtime information. (The object-cache-size statement is used to set the memory allocated for runtime services.) The following information is also displayed: <ul style="list-style-type: none"> Memory Alarm (zone): If the amount of free memory goes below the limit (64 MB for 32-bit Junos OS and 128 MB for 64-bit Junos OS), an overload alert (OVLD) is displayed. If not, then nothing is displayed. Percentage of the total number of bytes used.
Policy bytes used	Total number of policy bytes used and the percentage used. Policy bytes is the amount of memory used for user configuration and correlates with the policy-db-size statement.
CPU Utilization	Percentage of CPU utilization per PIC. The following information is also displayed: <ul style="list-style-type: none"> CPU Alarm (Zone): If the CPU utilization goes above the configured limit, then an overload alert (OVLD) is displayed. If not, then nothing is displayed.

Sample Output

```

show services user@host> show services service-sets summary
service-sets summary
Service sets
CPU
Interface    configured      Bytes used    Policy bytes used    utilization

```

ms-0/0/0	1	385021900	(81.96%)	299796 (0.44%)	92.89 % OVLD
----------	---	-----------	----------	-----------------	--------------

show services sessions (Aggregated Multiservices)

Syntax	<pre>show services sessions <brief extensive terse> <application-protocol <i>protocol</i>> <count> <destination-port <i>destination-port</i>> <destination-prefix <i>destination-prefix</i>> <interface <i>interface-name</i>> <limit <i>number</i>> <protocol <i>protocol</i>> <service-set <i>service-set</i>> <source-port <i>source-port</i>> <source-prefix <i>source-prefix</i>></pre>
Release Information	<p>Command introduced in Junos OS Mobility Release 10.4.</p> <p>Support for aggregated multiservices (AMS) introduced in Junos OS Mobility Release 11.2W.</p>
Description	Display the session information for each service set in each member interface of the AMS interface.
Options	<p>none—Display standard information about all sessions.</p> <p>brief extensive terse—(Optional) Display the specified level of output.</p> <p>application-protocol—(Optional) Display information about one of the following application protocols:</p> <ul style="list-style-type: none"> • ftp—File Transfer Protocol • icmp—Internet Control Message Protocol • pptp—Point-to-Point Tunneling Protocol • rtsp—Real-Time Streaming Protocol • sqlnet—SQL *Net • tcp—Transmission Control Protocol • traceroute—Traceroute • tftp—Trivial File Transfer Protocol • udp—User Datagram Protocol <p>count—(Optional) Display a count of the matching entries.</p> <p>destination-port <i>destination-port</i>—(Optional) Display information for a particular destination port. The range of values is from 0 through 65,535.</p> <p>destination-prefix <i>destination-prefix</i>—(Optional) Display information for a particular destination prefix.</p>

interface *interface-name*—(Optional) Display information about a particular interface.
On M Series and T Series routers, *interface-name* can be **ms-fpc/pic/port** or **rspnumber**.
On J Series routers, *interface-name* is **ms-pim/0/port**.

limit *number*—(Optional) Maximum number of entries to display.

protocol *protocol*—(Optional) Display information about one of the following IP types:

- **number**—Numeric protocol value from 0 through 255
- **ah**—IPsec Authentication Header protocol
- **egp**—An exterior gateway protocol
- **esp**—IPsec Encapsulating Security Payload protocol
- **gre**—A generic routing encapsulation protocol
- **icmp**—Internet Control Message Protocol
- **icmp6**—Internet Control Message Protocol version 6
- **igmp**—Internet Group Management Protocol
- **ipip**—IP-over-IP encapsulation protocol
- **ospf**—Open Shortest Path First protocol
- **pim**—Protocol Independent Multicast protocol
- **rsvp**—Resource Reservation Protocol
- **sctp**—Stream Control Transmission Protocol
- **tcp**—Transmission Control Protocol
- **udp**—User Datagram Protocol

service-set *service-set*—(Optional) Display information for a particular service set.

source-port *source-port*—(Optional) Display information for a particular source port. The range of values is from 0 through 65,535.

source-prefix *source-prefix*—(Optional) Display information for a particular source prefix.

Required Privilege Level	view
List of Sample Output	show services sessions brief on page 1263 show services sessions interface mams-5/0/0 extensive on page 1264 show services sessions terse on page 1266 show services sessions count on page 1267
Output Fields	Table 107 on page 1263 lists the output fields for the show services sessions command. Output fields are listed in the approximate order in which they appear.

Table 107: show services sessions Output Fields

Field Name	Field Description
Interface	Name of the member interface (mams-) and the aggregated multiservices interface (ams) to which it belongs.
Session ID	Session ID that uniquely identifies the session.
ALG	Name of the application.
Flags	Session flag for the ALG: <ul style="list-style-type: none"> • 0x1—Found an existing session. • 0x2—Reached session or flow limit. • 0x3—No memory available for new sessions. • 0x4—No free session ID available.
IP Action	Flag indicating whether IP action has been set for the session.
Offload	Flag indicating whether the session has been offloaded to the Packet Forwarding Engine.
Asymmetric	Flag indicating whether the session is unidirectional.
Service set	Name of a service set. Individual empty service sets are not displayed.
Sessions Count	Number of sessions.
Flow or Flow Prot	Protocol used for this session.
Source	Source prefix of the flow in the format source-prefix:port . For ICMP flows, port information is not displayed.
Dest	Destination prefix of the flow. For ICMP flows, port information is not displayed.
State	Status of the flow: <ul style="list-style-type: none"> • Drop—Drop all packets in the flow without response. • Forward—Forward the packet in the flow without looking at it. • Reject—Drop all packets in the flow with response. • Watch—Inspect packets in the flow. • Bypass—Bypass packets in the flow. • Unknown—Unknown flow status.
Packet Direction	Direction of the flow: ingress (I), egress (O), or unknown.
Frm count	Number of frames in the flow.

Sample Output

```
show services sessions user@host> show services sessions brief
brief
```

**show services sessions
interface mams-5/0/0
extensive**

```

mams-1/0/0 (ams0)
Service Set: napt_set, Session: 16777217, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no
UDP      30.30.30.2:63    ->    40.40.40.2:63    Forward I      85689
UDP      40.40.40.2:63    ->    30.30.30.160:6000 Forward 0      0

user@host> show services sessions interface mams-5/0/0 extensive
mams-1/0/0 (ams0)
Service Set: napt_set, Session: 16777235, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no
NAT Plugin Data:
  NAT Action: Translation Type - NAPT-44
  NAT source  30.30.30.62:63    ->    30.30.30.176:6003
UDP      30.30.30.62:63    ->    40.40.40.62:63    Forward I      1805
  Byte count: 83030
  Flow role: Initiator, Timeout: 0
UDP      40.40.40.62:63    ->    30.30.30.176:6003 Forward 0      0
  Byte count: 0
  Flow role: Responder, Timeout: 0
Service Set: napt_set, Session: 16777234, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no
NAT Plugin Data:
  NAT Action: Translation Type - NAPT-44
  NAT source  30.30.30.57:63    ->    30.30.30.163:6003
UDP      30.30.30.57:63    ->    40.40.40.57:63    Forward I      1805
  Byte count: 83030
  Flow role: Initiator, Timeout: 0
UDP      40.40.40.57:63    ->    30.30.30.163:6003 Forward 0      0
  Byte count: 0
  Flow role: Responder, Timeout: 0

[...output truncated...]
mams-1/1/0 (ams0)
Service Set: napt_set, Session: 16777234, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no
NAT Plugin Data:
  NAT Action: Translation Type - NAPT-44
  NAT source  30.30.30.63:63    ->    30.30.30.165:6004
UDP      30.30.30.63:63    ->    40.40.40.63:63    Forward I      1805
  Byte count: 83030
  Flow role: Initiator, Timeout: 0
UDP      40.40.40.63:63    ->    30.30.30.165:6004 Forward 0      0
  Byte count: 0
  Flow role: Responder, Timeout: 0
Service Set: napt_set, Session: 16777233, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no
NAT Plugin Data:
  NAT Action: Translation Type - NAPT-44
  NAT source  30.30.30.60:63    ->    30.30.30.164:6004
UDP      30.30.30.60:63    ->    40.40.40.60:63    Forward I      1805
  Byte count: 83030
  Flow role: Initiator, Timeout: 0
UDP      40.40.40.60:63    ->    30.30.30.164:6004 Forward 0      0
  Byte count: 0
  Flow role: Responder, Timeout: 0
Service Set: napt_set, Session: 16777232, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no

```

[...output truncated...]

mams-5/0/0 (ams0)

Service Set: napt_set, Session: 16777225, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no

NAT Pugin Data:

```

NAT Action: Translation Type - NAPT-44
NAT source 30.30.30.64:63 -> 30.30.30.168:6002
UDP 30.30.30.64:63 -> 40.40.40.64:63 Forward I 1805
Byte count: 83030
Flow role: Initiator, Timeout: 0
UDP 40.40.40.64:63 -> 30.30.30.168:6002 Forward 0 0
Byte count: 0
Flow role: Responder, Timeout: 0
Service Set: napt_set, Session: 16777224, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no

```

NAT Pugin Data:

```

NAT Action: Translation Type - NAPT-44
NAT source 30.30.30.56:63 -> 30.30.30.171:6001
UDP 30.30.30.56:63 -> 40.40.40.56:63 Forward I 1805
Byte count: 83030
Flow role: Initiator, Timeout: 0
UDP 40.40.40.56:63 -> 30.30.30.171:6001 Forward 0 0
Byte count: 0
Flow role: Responder, Timeout: 0
Service Set: napt_set, Session: 16777223, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no

```

[...output truncated...]

mams-5/1/0 (ams0)

Service Set: napt_set, Session: 16777233, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no

NAT Pugin Data:

```

NAT Action: Translation Type - NAPT-44
NAT source 30.30.30.61:63 -> 30.30.30.172:6004
UDP 30.30.30.61:63 -> 40.40.40.61:63 Forward I 1805
Byte count: 83030
Flow role: Initiator, Timeout: 0
UDP 40.40.40.61:63 -> 30.30.30.172:6004 Forward 0 0
Byte count: 0
Flow role: Responder, Timeout: 0
Service Set: napt_set, Session: 16777232, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no

```

NAT Pugin Data:

```

NAT Action: Translation Type - NAPT-44
NAT source 30.30.30.52:63 -> 30.30.30.175:6003
UDP 30.30.30.52:63 -> 40.40.40.52:63 Forward I 1805
Byte count: 83030
Flow role: Initiator, Timeout: 0
UDP 40.40.40.52:63 -> 30.30.30.175:6003 Forward 0 0
Byte count: 0
Flow role: Responder, Timeout: 0
Service Set: napt_set, Session: 16777231, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no

```

[...output truncated...]

```

user@router> show services sessions terse
mams-1/0/0 (ams0)
Service Set: napt_set, Session: 16777235, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no
UDP      30.30.30.62:63 -> 40.40.40.62:63 Forward I      2541
UDP      40.40.40.62:63 -> 30.30.30.176:6003 Forward O      0
Service Set: napt_set, Session: 16777234, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no
UDP      30.30.30.57:63 -> 40.40.40.57:63 Forward I      2541
UDP      40.40.40.57:63 -> 30.30.30.163:6003 Forward O      0
Service Set: napt_set, Session: 16777233, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no
UDP      30.30.30.50:63 -> 40.40.40.50:63 Forward I      2541
UDP      40.40.40.50:63 -> 30.30.30.162:6003 Forward O      0
Service Set: napt_set, Session: 16777232, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no
UDP      30.30.30.48:63 -> 40.40.40.48:63 Forward I      2541
UDP      40.40.40.48:63 -> 30.30.30.161:6003 Forward O      0
[...output truncated...]
mams-1/1/0 (ams0)
Service Set: napt_set, Session: 16777234, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no
UDP      30.30.30.63:63 -> 40.40.40.63:63 Forward I      2543
UDP      40.40.40.63:63 -> 30.30.30.165:6004 Forward O      0
Service Set: napt_set, Session: 16777233, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no
UDP      30.30.30.60:63 -> 40.40.40.60:63 Forward I      2543
UDP      40.40.40.60:63 -> 30.30.30.164:6004 Forward O      0
Service Set: napt_set, Session: 16777232, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no
UDP      30.30.30.59:63 -> 40.40.40.59:63 Forward I      2543
UDP      40.40.40.59:63 -> 30.30.30.167:6003 Forward O      0
Service Set: napt_set, Session: 16777231, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no
UDP      30.30.30.58:63 -> 40.40.40.58:63 Forward I      2543
UDP      40.40.40.58:63 -> 30.30.30.166:6003 Forward O      0
[...output truncated...]
mams-5/0/0 (ams0)
Service Set: napt_set, Session: 16777225, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no
UDP      30.30.30.64:63 -> 40.40.40.64:63 Forward I      2543
UDP      40.40.40.64:63 -> 30.30.30.168:6002 Forward O      0
Service Set: napt_set, Session: 16777224, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no
UDP      30.30.30.56:63 -> 40.40.40.56:63 Forward I      2543
UDP      40.40.40.56:63 -> 30.30.30.171:6001 Forward O      0
Service Set: napt_set, Session: 16777223, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no
UDP      30.30.30.55:63 -> 40.40.40.55:63 Forward I      2543
UDP      40.40.40.55:63 -> 30.30.30.170:6001 Forward O      0
Service Set: napt_set, Session: 16777222, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no
UDP      30.30.30.51:63 -> 40.40.40.51:63 Forward I      2543
UDP      40.40.40.51:63 -> 30.30.30.169:6001 Forward O      0
[...output truncated...]
mams-5/1/0 (ams0)
Service Set: napt_set, Session: 16777233, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no
UDP      30.30.30.61:63 -> 40.40.40.61:63 Forward I      2544
UDP      40.40.40.61:63 -> 30.30.30.172:6004 Forward O      0
Service Set: napt_set, Session: 16777232, ALG: none, Flags: 0x2000, IP Action:

```



```

no, Offload: no, Asymmetric: no
UDP      30.30.30.52:63  ->  40.40.40.52:63  Forward I      2545
UDP      40.40.40.52:63  ->  30.30.30.175:6003 Forward 0        0
Service Set: napt_set, Session: 16777231, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no
UDP      30.30.30.47:63  ->  40.40.40.47:63  Forward I      2545
UDP      40.40.40.47:63  ->  30.30.30.174:6003 Forward 0        0
Service Set: napt_set, Session: 16777230, ALG: none, Flags: 0x2000, IP Action:
no, Offload: no, Asymmetric: no
UDP      30.30.30.46:63  ->  40.40.40.46:63  Forward I      2545
UDP      40.40.40.46:63  ->  30.30.30.173:6003 Forward 0        0
[...output truncated...]

```

```

show services sessions count user@host> show services sessions count
count Interface Service set Sessions count
mams-1/0/0 napt_set 19
mams-1/0/0 ssl 0
mams-1/1/0 napt_set 18
mams-1/1/0 ssl 0
mams-5/0/0 napt_set 9
mams-5/0/0 ssl 0
mams-5/1/0 napt_set 17
mams-5/1/0 ssl 0

```


CHAPTER 37

System Architecture Operational Commands

clear unified-edge sgw idle-mode-buffering statistics

Syntax	clear unified-edge sgw idle-mode-buffering statistics <all> <fpc-slot <i>fpc-slot</i>> <gateway <i>gateway</i>> <pic-slot <i>pic-slot</i>>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Clear the idle mode buffering statistics for one or more Serving Gateways (S-GWs). If a gateway name is not specified, then statistics for all S-GWs are cleared.
Options	none —Clear the idle mode buffering statistics for all S-GWs. all —(Optional) Clear all the buffering statistics including the idle mode buffering statistics and the statistics collected during the initial bearer setup. fpc-slot <i>fpc-slot</i> pic-slot <i>pic-slot</i> —(Optional) Clear the idle mode buffering statistics for the specified Flexible PIC Concentrator (FPC) and PIC slot numbers. gateway —(Optional) Clear the idle mode buffering statistics for all the services PICs in the specified gateway.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show unified-edge sgw idle-mode-buffering statistics on page 1286
List of Sample Output	clear unified-edge sgw idle-mode-buffering statistics on page 1270
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear unified-edge sgw idle-mode-buffering statistics	<pre>user@host> clear unified-edge sgw idle-mode-buffering statistics Cleared idle mode buffering statistics</pre>
--	---

clear unified-edge sgw statistics

Syntax	clear unified-edge sgw statistics gateway <i>gateway-name</i>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Clear all the statistics for the specified Serving Gateway (S-GW).
Options	gateway <i>gateway-name</i> —Clear the statistics for the specified S-GW.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show unified-edge sgw statistics on page 1292
List of Sample Output	clear unified-edge sgw statistics gateway SGW on page 1271
Output Fields	No message is displayed on successful execution of this command; otherwise an error message is displayed.

Sample Output

clear unified-edge sgw statistics gateway SGW	user@host> clear unified-edge sgw statistics gateway SGW
---	--


clear unified-edge sgw subscribers

Syntax	<code>clear unified-edge sgw subscribers gateway <i>gateway</i></code> <code><imsi <i>imsi</i>></code> <code><msisdn <i>msisdn</i>></code>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Clear the subscribers for the Serving Gateway (S-GW) based on the options specified.
Options	<p>gateway <i>gateway</i>—Clear the subscribers for the specified S-GW.</p> <p>imsi <i>imsi</i>—(Optional) Clear the subscriber matching the specified International Mobile Subscriber Identity (IMSI).</p> <p>msisdn <i>msisdn</i>—(Optional) Clear the subscriber matching the specified Mobile Station ISDN (MSISDN) number.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• clear unified-edge sgw subscribers charging on page 1273• clear unified-edge sgw subscribers peer on page 1274• show unified-edge sgw subscribers on page 1300
List of Sample Output	clear unified-edge sgw subscribers gateway SGW on page 1272
Output Fields	No message is displayed on successful execution of this command; otherwise an error message is displayed.

Sample Output

clear unified-edge sgw subscribers gateway SGW	user@host> clear unified-edge sgw subscribers gateway SGW
--	---

clear unified-edge sgw subscribers charging

Syntax	<code>clear unified-edge sgw subscribers charging gateway <i>gateway</i></code> <code><charging-profile <i>charging-profile</i>></code> <code><transport-profile <i>transport-profile</i>></code>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Clear the charging information for subscribers on the Serving Gateway (S-GW) based on the options specified.
Options	<p>gateway <i>gateway</i>—Clear the charging information for all subscribers for the specified S-GW.</p> <p>charging-profile <i>charging-profile</i>—(Optional) Clear the subscriber matching the specified charging profile name.</p> <p>transport-profile <i>transport-profile</i>—(Optional) Clear the subscriber matching the specified transport profile name.</p>
<div>  <p>NOTE: You must specify either a charging profile or a transport profile to run this command.</p> </div>	
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • clear unified-edge sgw subscribers on page 1272 • show unified-edge sgw subscribers on page 1300 • clear unified-edge sgw subscribers peer on page 1274
List of Sample Output	clear unified-edge sgw subscribers charging gateway SGW on page 1273
Output Fields	No message is displayed on successful execution of this command; otherwise an error message is displayed.

Sample Output

```
clear unified-edge sgw subscribers charging gateway SGW
user@host> clear unified-edge sgw subscribers charging gateway SGW
```

clear unified-edge sgw subscribers peer

Syntax	<code>clear unified-edge sgw subscribers peer gateway <i>gateway</i> remote-addr <i>remote-addr</i> <local-addr <i>local-addr</i>> <routing-instance <i>routing-instance</i>></code>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Clear the information for subscribers anchored for the specified GPRS tunneling protocol (GTP) peer. The GTP peer can be an S4 Serving GPRS Support Node (S4-SGSN), Mobility Management Entity (MME), or a Packet Data Network Gateway (P-GW).
Options	<p>gateway <i>gateway</i>—Clear the subscribers for the specified gateway.</p> <p>remote-addr <i>remote-addr</i>—Clear the information for subscribers anchored on the peer with the specified IPv4 address.</p> <p>local-addr <i>local-addr</i>—(Optional) Clear the subscriber matching the specified local IPv4 address of the broadband gateway on that interface.</p> <p>routing-instance <i>routing-instance</i>—(Optional) Clear the subscriber matching the specified routing instance.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• clear unified-edge sgw subscribers on page 1272• clear unified-edge sgw subscribers charging on page 1273• show unified-edge sgw subscribers on page 1300
List of Sample Output	clear unified-edge sgw subscribers peer gateway pgw remote-addr 11.11.11.2 on page 1274
Output Fields	No message is displayed on successful execution of this command; otherwise an error message is displayed.

Sample Output

```
clear unified-edge sgw subscribers peer
gateway pgw
remote-addr 11.11.11.2
```

```
user@host> clear unified-edge sgw subscribers peer gateway pgw remote-addr 11.11.11.2
```


show unified-edge gateways

Syntax	show unified-edge gateways <brief detail>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Display information about all gateways configured on the chassis.
Options	none —(Same as brief) Display information about the configured gateways in brief. brief detail —(Optional) Display the specified level of output.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show unified-edge ggsn-pgw system interfaces on page 1066 • show unified-edge sgw system interfaces on page 1068
List of Sample Output	show unified-edge gateways brief on page 1276 show unified-edge gateways detail on page 1276
Output Fields	Table 108 on page 1275 lists the output fields for the show unified-edge gateways command. Output fields are listed in the approximate order in which they appear.

Table 108: show unified-edge gateways Field Descriptions

Field Name	Field Description	Level of Output
Gateway name	Name of the gateway.	All levels
Gateway type	Type of gateway: <ul style="list-style-type: none"> • ggsn-pgw—Gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW). • sgw—Serving Gateway (S-GW). 	All levels
Gateway ID	Internal ID of the gateway.	All levels
Gateway uplink mif interface	Mobile interface, on the gateway, used for uplink packets.	detail
Gateway downlink mif interface	Mobile interface, on the gateway, used for downlink packets.	detail
Gateway anchor-pfe interface	Packet Forwarding Engine interfaces (pfe-) or anchor Packet Forwarding Engine interfaces (apfe-) configured on the gateway.	detail
Gateway anchor-spic interface	Multiservices interfaces (ms-) or aggregated multiservices interfaces (ams-) configured on the gateway.	detail

Sample Output

show unified-edge gateways brief user@host> show unified-edge gateways brief

Total number of configured gateways: 2

Gateway name: PGW
Gateway type: ggsn-pgw
Gateway id: 1

Gateway name: SGW
Gateway type: sgw
Gateway id: 2

show unified-edge gateways detail user@host> show unified-edge gateways detail

Total number of configured gateways: 2

Gateway name: PGW
Gateway type: ggsn-pgw
Gateway id: 1
Gateway uplink mif interface: mif.64001
Gateway downlink mif interface: ---
Gateway anchor-pfe interfaces: pfe-5/0/0
Gateway anchor-spic interfaces: ms-3/0/0

Gateway name: SGW
Gateway type: sgw
Gateway id: 2
Gateway uplink mif interface: mif.64003
Gateway downlink mif interface: mif.64004
Gateway anchor-pfe interfaces: pfe-0/0/0
Gateway anchor-spic interfaces: ms-1/0/0

show unified-edge ggsn-pgw call-rate statistics

Syntax	<code>show unified-edge ggsn-pgw call-rate statistics</code> <code><gateway gateway-name></code> <code><history></code>
Release Information	Command introduced in Junos OS Mobility Release 11.2W. <code>gateway</code> option introduced in Junos OS Mobility Release 11.4W.
Description	Display the call-rate statistics for one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then information for all GGSNs and P-GWs is displayed.
Options	<p>none—Display the call-rate statistics for all GGSNs or P-GWs.</p> <p>gateway gateway-name—(Optional) Display the call-rate statistics for the specified GGSN or P-GW.</p> <p>history—(Optional) Display the call-rate statistics for a specified number of past intervals. (The number of past intervals is configured using the <code>set call-rate-statistics history</code> statement at the <code>[edit unified-edge gateways ggsn-pgw gateway-name]</code> hierarchy level.)</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> call-rate-statistics on page 981
List of Sample Output	show unified-edge ggsn-pgw call-rate statistics on page 1278 show unified-edge ggsn-pgw call-rate statistics history on page 1278
Output Fields	Table 109 on page 1277 lists the output fields for the <code>show unified-edge ggsn-pgw call-rate statistics</code> command. Output fields are listed in the approximate order in which they appear.

Table 109: show unified-edge ggsn-pgw call-rate statistics Output Fields

Field Name	Field Description
Gateway	Name of the GGSN or P-GW.
Record	Record number for the interval in which the call-rate statistics are collected, starting from the newest record (1) to the oldest.
Call-rate interval	Interval, in minutes, for which the call-rate statistics are calculated.
Control Plane	<p>The following control plane information is displayed:</p> <ul style="list-style-type: none"> Activations—Number of activations during the call-rate interval. Deactivations—Number of deactivations during the call-rate interval.

Table 109: show unified-edge ggsn-pgw call-rate statistics Output Fields (*continued*)

Field Name	Field Description
Data Plane (Gn)	<p>The following data plane (Gn interface) information is displayed:</p> <ul style="list-style-type: none"> • Input packets—Number of data packets received during the call-rate interval. • Output packets—Number of data packets transmitted during the call-rate interval. • Input bytes—Number of data bytes received during the call-rate interval. • Output bytes—Number of data bytes transmitted during the call-rate interval.
Statistics collection time	Date and time when the call-rate statistics for the record are computed.

Sample Output

```

show unified-edge ggsn-pgw call-rate statistics
user@host> show unified-edge ggsn-pgw call-rate statistics
Gateway: PGW
Record 1 (Call-rate statistics for the past 5 min):
Control Plane:
    Activations:    0
    Deactivations: 0
Data Plane(Gn):
    Input Packets:  0
    Output packets: 0
    Input bytes:    0
    Output bytes:   0
Statistics collection time: 2011-10-18 05:29:36 PDT (00:04:01 ago)

Gateway: PGW2
Record 1 (Call-rate statistics for the past 5 min):
Control Plane:
    Activations:    0
    Deactivations: 0
Data Plane(Gn):
    Input Packets:  0
    Output packets: 0
    Input bytes:    0
    Output bytes:   0
Statistics collection time: 2011-10-18 05:29:36 PDT (00:04:01 ago)

show unified-edge ggsn-pgw call-rate statistics history
user@host> show unified-edge ggsn-pgw call-rate statistics history
Gateway: PGW
Record 1 (Call-rate statistics for the past 5 min):
Control Plane:
    Activations:    0
    Deactivations: 0
Data Plane(Gn):
    Input Packets:  0
    Output packets: 0
    Input bytes:    0
    Output bytes:   0

```

Statistics collection time: 2011-10-18 05:29:36 PDT (00:04:03 ago)

Record 2 (Call-rate statistics for the past 5 min):

Control Plane:

Activations: 0

Deactivations: 0

Data Plane(Gn):

Input Packets: 0

Output packets: 0

Input bytes: 0

Output bytes: 0

Statistics collection time: 2011-10-18 05:24:36 PDT (00:09:03 ago)

Record 3 (Call-rate statistics for the past 5 min):

Control Plane:

Activations: 0

Deactivations: 0

Data Plane(Gn):

Input Packets: 0

Output packets: 0

Input bytes: 0

Output bytes: 0

Statistics collection time: 2011-10-18 05:19:36 PDT (00:14:03 ago)

Gateway: PGW2

Record 1 (Call-rate statistics for the past 5 min):

Control Plane:

Activations: 0

Deactivations: 0

Data Plane(Gn):

Input Packets: 0

Output packets: 0

Input bytes: 0

Output bytes: 0

Statistics collection time: 2011-10-18 05:29:36 PDT (00:04:03 ago)

Record 2 (Call-rate statistics for the past 5 min):

Control Plane:

Activations: 0

Deactivations: 0

Data Plane(Gn):

Input Packets: 0

Output packets: 0

Input bytes: 0

Output bytes: 0

Statistics collection time: 2011-10-18 05:24:36 PDT (00:09:03 ago)

show unified-edge ggsn-pgw resource-manager clients

Syntax	show unified-edge ggsn-pgw resource-manager clients <gateway gateway>
Release Information	Command introduced in Junos OS Mobility Release 11.2W. gateway option introduced in Junos OS Mobility Release 11.4W.
Description	Display information about the resource management clients (the session Dense Port Concentrators [DPCs] and interface DPCs and Modular Port Concentrators [MPCs]) on one or more gateway GPRS support nodes (GGSNs) or Packet Data Network Gateways (P-GWs). If a GGSN or P-GW is not specified, then information for all GGSNs and P-GWs is displayed.
Options	none —Display information for one or more GGSNs or P-GWs. gateway gateway-name —(Optional) Display information for the specified gateway.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show unified-edge gateways on page 1275 • show unified-edge ggsn-pgw system interfaces on page 1066
List of Sample Output	show unified-edge ggsn-pgw resource-manager clients on page 1281
Output Fields	Table 110 on page 1280 lists the output fields for the show unified-edge gateways ggsn-pgw resource-manager clients command. Output fields are listed in the approximate order in which they appear.

Table 110: show unified-edge gateways ggsn-pgw resource-manager clients Output Fields

Field Name	Field Description
Client	Name of the resource manager client slot identified by the FPC and PIC slot numbers; for example, pfe-1/2/0 or ms/7/0/0 .
State	Resource manager client state. In-Service means that the client can handle session creation requests.
Role	Role of the resource manager client slot: <ul style="list-style-type: none"> • Primary—The resource manager client is a primary member. • Secondary—The resource manager client is a secondary or backup member.
Client type	Type of resource manager client: <ul style="list-style-type: none"> • Anchor PFE—Packet Forwarding Engine client used for anchoring subscribers in the gateway. • Session PIC—Session PIC client used for the mobile control plane in the gateway • Service PIC—services PIC used for anchoring services-related subscriber sessions in the gateway
Gateway	Name of the gateway to which the resource manager client belongs.

Sample Output

```

show unified-edge user@host> show unified-edge ggsn-pgw resource-manager clients
ggsn-pgw          Client      State      Redundancy role Client type Gateway
resource-manager  ms-0/0/0    In-Service Secondary    Session-PIC PGW
clients           ms-0/1/0    In-Service Primary      Session-PIC PGW
                  pfe-1/0/0   In-Service Primary      Anchor-PFE  PGW
                  pfe-1/2/0   In-Service Primary      Anchor-PFE  PGW
                  pfe-2/0/0   In-Service Primary      Anchor-PFE  PGW
                  pfe-2/3/0   In-Service Primary      Anchor-PFE  PGW
                  pfe-3/0/0   In-Service Secondary   Anchor-PFE  PGW
                  pfe-3/2/0   In-Service Secondary   Anchor-PFE  PGW
                  pfe-4/0/0   In-Service Primary      Anchor-PFE  PGW
                  pfe-4/2/0   In-Service Primary      Anchor-PFE  PGW
                  ms-5/0/0    In-Service Primary      Session-PIC PGW
                  ms-5/1/0    In-Service Primary      Session-PIC PGW

```

show unified-edge sgw call-rate statistics

Syntax	show unified-edge sgw call-rate statistics <gateway gateway-name> <history>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Display the call-rate statistics for one or more Serving Gateways (S-GWs). If a gateway is not specified, then information for all S-GWs is displayed.
Options	<p>none—Display the call-rate statistics for all S-GWs.</p> <p>gateway gateway-name—(Optional) Display the call-rate statistics for the specified gateway.</p> <p>history—(Optional) Display the call-rate statistics for a specified number of past intervals. (The number of past intervals is configured using the set call-rate-statistics history statement at the [edit unified-edge gateways sgw gateway-name] hierarchy level.)</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> call-rate-statistics on page 981
List of Sample Output	show unified-edge sgw call-rate statistics on page 1283 show unified-edge sgw call-rate statistics history on page 1283
Output Fields	Table 111 on page 1282 lists the output fields for the show unified-edge sgw call-rate statistics command. Output fields are listed in the approximate order in which they appear.

Table 111: show unified-edge sgw call-rate statistics Output Fields

Field Name	Field Description
Gateway	Name of the S-GW.
Record	Record number for the interval in which the call-rate statistics are collected, starting from the newest record (1) to the oldest.
Call-rate interval	Interval, in minutes, for which the call-rate statistics are calculated.
Control Plane	<p>The following control plane information is displayed:</p> <ul style="list-style-type: none"> Activations—Number of activations during the call-rate interval. Deactivations—Number of deactivations during the call-rate interval.

Table 111: show unified-edge sgw call-rate statistics Output Fields (*continued*)

Field Name	Field Description
Data Plane (Gn)	<p>The following data plane (Gn interface) information is displayed:</p> <ul style="list-style-type: none"> • Input packets—Number of data packets received during the call-rate interval. • Output packets—Number of data packets transmitted during the call-rate interval. • Input bytes—Number of data bytes received during the call-rate interval. • Output bytes—Number of data bytes transmitted during the call-rate interval.
Statistics collection time	Date and time when the call-rate statistics for the record are computed.

Sample Output

```

show unified-edge sgw call-rate statistics user@host> show unified-edge sgw call-rate statistics
Gateway: SGW
Record 1 (Call-rate statistics for the past 10 min):
Control Plane:
    Activations:    1
    Deactivations: 0
Data Plane(Gn):
    Input Packets:  0
    Output packets: 2
    Input bytes:    0
    Output bytes:   584
Statistics collection time: 2011-12-09 21:08:30 PST (00:00:49 ago)

```

```

show unified-edge sgw call-rate statistics history user@host> show unified-edge sgw call-rate statistics history
Gateway: SGW
Record 1 (Call-rate statistics for the past 10 min):
Control Plane:
    Activations:    1
    Deactivations: 0
Data Plane(Gn):
    Input Packets:  0
    Output packets: 2
    Input bytes:    0
    Output bytes:   584
Statistics collection time: 2011-12-09 21:08:30 PST (00:01:17 ago)

```

show unified-edge sgw service-mode

Syntax	show unified-edge sgw service-mode <brief detail> <gateway gateway-name>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Display the service mode information for one or more Serving Gateways (S-GWs). If a gateway is not specified, then information for all S-GWs is displayed.
Options	<p>none—(Same as brief) Display the service mode information in brief.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>gateway gateway-name—(Optional) Display the service mode information for the specified gateway.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> service-mode (Serving Gateway) on page 916
List of Sample Output	show unified-edge sgw service-mode brief on page 1284 show unified-edge sgw service-mode detail on page 1285
Output Fields	Table 87 on page 1162 lists the output fields for the show unified-edge sgw service-mode command. Output fields are listed in the approximate order in which they appear.

Table 112: show unified-edge sgw service-mode Output Fields

Field Name	Field Description	Level of Output
Gateway Name	Name of the S-GW.	All levels
Service Mode	Service mode for the gateway: <ul style="list-style-type: none"> Operational—Gateway is in operational mode. Maintenance—Gateway is in maintenance mode. 	All levels

Sample Output

```

user@host> show unified-edge sgw service-mode brief
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

```

SGW	Operational
SGW2	Operational

```
show unified-edge sgw service-mode detail
user@host> show unified-edge sgw service-mode detail
Service Mode Status
Gateway Name    : SGW
Service Mode    : Operational
Service Mode Status
Gateway Name    : SGW2
Service Mode    : Operational
```

show unified-edge sgw idle-mode-buffering statistics

Syntax `show unified-edge sgw idle-mode-buffering statistics`
`<brief | detail>`
`<fpc-slot fpc-slot>`
`<gateway gateway>`
`<pic-slot pic-slot>`

Release Information Command introduced in Junos OS Mobility Release 11.4W.

Description Display the idle mode buffering statistics for one or more Serving Gateways (S-GWs). If a gateway name is not specified, then statistics for all S-GWs are displayed.

Options **none**—(Same as brief) Display the idle mode buffering statistics for all S-GWs.
brief | detail—(Optional) Display the specified level of output.



NOTE: The **brief** option displays the aggregated statistics from all the services PICs for each S-GW. The **detail** option displays the statistics for each services PIC separately for each S-GW.

fpc-slot fpc-slot pic-slot pic-slot—(Optional) Display the idle mode buffering statistics for the specified Flexible PIC Concentrator (FPC) and PIC slot numbers.

gateway—(Optional) Display the idle mode buffering statistics for all the services PICs in the specified gateway.

Required Privilege Level view

Related Documentation • [clear unified-edge sgw idle-mode-buffering statistics on page 1270](#)

List of Sample Output [show unified-edge sgw idle-mode-buffering statistics brief on page 1288](#)
[show unified-edge sgw idle-mode-buffering statistics detail on page 1289](#)

Output Fields [Table 113 on page 1286](#) lists the output fields for the **show unified-edge sgw idle-mode-buffering statistics** command. Output fields are listed in the approximate order in which they appear.

Table 113: show unified-edge sgw idle-mode-buffering statistics Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the S-GW.	All levels
FPC Slot	FPC slot number for which the statistics are displayed.	detail
PIC slot	PIC slot number for which the statistics are displayed.	detail

Table 113: show unified-edge sgw idle-mode-buffering statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
Idle Mode Buffering Statistics: —The following idle mode buffering statistics related to GTPv1 downlink are displayed.		
Total Packets received	Total number of packets received from the Packet Forwarding Engine for idle subscribers.	All levels
Invalid packets	Total number of packets received that failed validation checks; these packets are received from the Packet Forwarding Engine.	All levels
Flows created	Total number of flows created to handle packets.	All levels
Flows aged out	Total number of flows aged out.	All levels
Active Flows	Number of current active flows.	All levels
Active Buffered Flows	Number of active flows that are currently being buffered.	All levels
Buffering Statistics —The following consolidated statistics are displayed for packets buffered for idle subscribers and for packets buffered during the initial bearer setup.		
Active Buffered Flows	Number of current active flows that are handling buffering for idle subscribers and for packets buffered during initial bearer setup.	All levels
Packets/Bytes	The following information about packets that need buffering is displayed: <ul style="list-style-type: none"> • Total Received—Total number of packets received from the Packet Forwarding Engine for idle subscribers and buffered during initial bearer setup. • Invalid—Total number of packets received that failed validation checks. • Current Buffered—Number of currently buffered packets and their size, in bytes. • Reinjected—Total number of packets reinjected to the Packet Forwarding Engine and their size, in bytes. • Dropped (Exceeded limit)—Total number of packets dropped because the buffering limit was exceeded and the size of the dropped packets, in bytes. • Buffered (Dropped)—Total number of buffered packets that were dropped and their size, in bytes. 	All levels

Table 113: show unified-edge sgw idle-mode-buffering statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
Limit Exceeded	<p>The following information about the number of times that the buffer and memory limits are exceeded is displayed:</p> <ul style="list-style-type: none"> • Dedicated buffer-limit—Number of times the dedicated buffer limit of 2 KB is exceeded. • Shared buffer-limit—Number of times the shared buffer limit of 10 KB is exceeded. • Dedicated memory-limit—Number of times the dedicated memory limit of 75 percent is exceeded. • Shared memory-limit—Number of times the shared memory limit of 25 percent is exceeded. 	All levels
Memory Usage	<p>The following information about memory usage is displayed:</p> <ul style="list-style-type: none"> • Memory used (Bytes)—Amount of dedicated and shared memory used, in bytes. • Memory free (Bytes)—Amount of free memory, in bytes. • Dedicated memory used (%)—Percentage of dedicated memory used. • Shared memory used (%)—Percentage of shared memory used. 	All levels

Sample Output

```
show unified-edge sgw idle-mode-buffering statistics brief
```

```
user@host> show unified-edge sgw idle-mode-buffering statistics brief
Gateway: SGW
```

```
Idle Mode Buffering statistics:
```

```
GTPv1 Downlink:
Total Packets received:      102
Invalid packets:             0
Flows created:               12
Flows aged out:              0
Active Flows:                10
Active Buffered Flows:       10
```

```
Buffering statistics:
```

```
Active Buffered Flows:      10
Packets/Bytes:
Total Received:             102
Invalid:                     0
Current Buffered:           100 / 16400
Reinjected:                  2 / 280
Dropped (Exceeded limit):   0 / 0
Buffered Dropped:           0 / 0
```

```
Limit Exceeded:
```

```
Dedicated buffer-limit:    0
Shared buffer-limit:        0
Dedicated memory-limit:    0
Shared memory-limit:        0
```

```
Memory Usage:
```

```
Memory used (Bytes):        7991432
Memory free (Bytes):        124129144
```

Dedicated memory used (%):	0
Shared memory used (%):	0

```
show unified-edge sgw idle-mode-buffering statistics detail
user@host> show unified-edge sgw idle-mode-buffering statistics detail
Gateway: SGW
```

Idle Mode Buffering statistics (FPC 0 PIC 0):

GTPv1 Downlink:

Total Packets received:	102
Invalid packets:	0
Flows created:	12
Flows aged out:	0
Active Flows:	0
Active Buffered Flows:	0

Buffering statistics (FPC 0 PIC 0):

Active Buffered Flows:	0
------------------------	---

Packets/Bytes:

Total Received:	102
Invalid:	0
Current Buffered:	0 / 0
Reinjected:	2 / 280
Dropped (Exceeded limit):	0 / 0
Buffered Dropped:	100 / 16400

Limit Exceeded:

Dedicated buffer-limit:	0
Shared buffer-limit:	0
Dedicated memory-limit:	0
Shared memory-limit:	0

Memory Usage:

Memory used (Bytes):	7954632
Memory free (Bytes):	124165944
Dedicated memory used (%):	0
Shared memory used (%):	0

show unified-edge sgw resource-manager clients

Syntax	show unified-edge sgw resource-manager clients <gateway gateway>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Display information about the resource management clients (the session Dense Port Concentrators [DPCs] and interface DPCs and Modular Port Concentrators [MPCs]) on one or more configured Serving Gateways (S-GWs). If a gateway is not specified, then information for all configured S-GWs is displayed.
Options	gateway gateway —(Optional) Display resource management information for the specified gateway.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show unified-edge gateways on page 1275 • show unified-edge sgw system interfaces on page 1068
List of Sample Output	show unified-edge sgw resource-manager clients on page 1291
Output Fields	Table 114 on page 1290 lists the output fields for the show unified-edge sgw resource-manager clients command. Output fields are listed in the approximate order in which they appear.

Table 114: show unified-edge sgw resource-manager clients Output Fields

Field Name	Field Description
Client	Name of the resource manager client slot identified by the FPC and PIC slot numbers; for example, pfe-1/2/0 or ms/7/0/0 .
State	Resource manager client state. In-Service means that the client can handle session creation requests.
Redundancy Role	Redundancy role of the resource manager client slot: <ul style="list-style-type: none"> • Primary—The resource manager client is a primary member. • Secondary—The resource manager client is a secondary or backup member.
Client type	Type of resource manager client: <ul style="list-style-type: none"> • Anchor PFE—Packet Forwarding Engine client used for anchoring subscribers in the gateway. • Session PIC—Session PIC client used for the mobile control plane in the gateway
Gateway	Name of the gateway to which the resource manager client belongs.

Sample Output

```

show unified-edge sgw resource-manager clients
user@host> show unified-edge sgw resource-manager clients
Client      State      Redundancy role Client type Gateway
ms-0/0/0    In-Service Primary     Session-PIC sgw.tokyo.kddi.com
ms-0/1/0    In-Service Primary     Session-PIC sgw.moscow.mts.com
ms-3/0/0    In-Service Primary     Session-PIC sgw.tokyo.kddi.com
ms-3/1/0    In-Service Primary     Session-PIC sgw.moscow.mts.com
pfe-5/0/0   In-Service Primary     Anchor-PFE  sgw.tokyo.kddi.com
pfe-5/1/0   In-Service Primary     Anchor-PFE  sgw.tokyo.kddi.com
pfe-5/2/0   In-Service Primary     Anchor-PFE  sgw.moscow.mts.com
pfe-5/3/0   In-Service Primary     Anchor-PFE  sgw.moscow.mts.com

```

show unified-edge sgw statistics

Syntax	show unified-edge sgw statistics <gateway gateway>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Display the statistics for one or more Serving Gateways (S-GWs). If a gateway name is not specified, then statistics for all S-GWs are displayed.
Options	none —Display statistics for all S-GWs. gateway gateway —(Optional) Display statistics for the specified gateway.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear unified-edge sgw statistics on page 1271
List of Sample Output	show unified-edge sgw statistics on page 1293
Output Fields	Table 115 on page 1292 lists the output fields for the show unified-edge sgw statistics command. Output fields are listed in the approximate order in which they appear.

Table 115: show unified-edge sgw statistics Output Fields

Field Name	Field Description
Gateway	Name of the S-GW.
Control Plane Statistics	
Session establishment attempts	Number of attempted session establishments.
Successful session establishments	Number of session successfully established.
Dedicated bearer creation attempts	Number of times the creation of dedicated bearers was attempted.
Successful dedicated bearer creations	Number of dedicated bearers successfully created.
Session deactivation attempts	Number of attempted session deactivations.
Successful session deactivations	Number of sessions successfully deactivated.
Dedicated bearer deactivation attempts	Number of times the deactivation of dedicated bearers was attempted.
Successful dedicated bearer deactivations	Number of dedicated bearers successfully deactivated.
Inter-RAT handover attempts	Number of Inter-RAT handovers attempted.
Inter-RAT handover successful	Number of successful Inter-RAT handovers.

Table 115: show unified-edge sgw statistics Output Fields (*continued*)

Field Name	Field Description
X2 based handover attempts	Number of X2-based handovers attempted.
X2 based handover successful	Number of successful X2-based handovers.
S1 based handover attempts	Number of S1-based handovers attempted.
S1 based handover successful	Number of successful S1-based handovers.
Data Plane GTP Statistics (S5/S8)	
Input packets	Number of incoming GTP data packets on the S5, and S8 interfaces.
Input bytes	Number of octets of incoming GTP data packets on the S5, and S8 interfaces.
Output packets	Number of outgoing GTP data packets on the S5, and S8 interfaces.
Output bytes	Number of octets of outgoing GTP data packets on the S5, and S8 interfaces.
Data plane GTP statistics (S4/S12/S1-U)	
Input packets	Number of incoming GTP data packets on the S1-U, S12, and S4 interfaces.
Input bytes	Number of octets of incoming GTP data packets on the S1-U, S12, and S4 interfaces.
Output packets	Number of outgoing GTP data packets on the S1-U, S12, and S4 interfaces.
Output bytes	Number of octets of outgoing GTP data packets on the S1-U, S12, and S4 interfaces.

Sample Output

```

show unified-edge sgw statistics user@host> show unified-edge sgw statistics
                                Gateway: SGW
                                Control plane statistics:
                                  Session establishment attempts:      2438203
                                  Successful session establishments:    2069870
                                  Dedicated bearer creation attempts:    0
                                  Successful dedicated bearer creations: 0
                                  Session deactivation attempts:        0
                                  Successful session deactivations:     0
                                  Dedicated bearer deactivation attempts: 0
                                  Successful dedicated bearer deactivations: 0
                                  Inter-RAT handover attempts:          0
                                  Inter-RAT handover successful:         0
                                  X2 based handover attempts:            197863
                                  X2 based handover successful:          197863
                                  S1 based handover attempts:            0
                                  S1 based handover successful:           0
                                Data plane GTP statistics (S5/S8):
                                  Input packets:                        292994029

```

```
Input    bytes:      37503235712
Output   packets:   298519448
Output   bytes:      38210489344
Data plane GTP statistics (S4/S12/S1-U):
Input    packets:   298519448
Input    bytes:      38210489344
Output   packets:   292994029
Output   bytes:      37503235712
```

show unified-edge sgw status

Syntax	<pre>show unified-edge sgw status <brief detail> <fpc-slot <i>fpc-slot</i>> <gateway <i>gateway</i>> <gtpv2-priority-level <i>gtpv2-priority-level</i>> <pic-slot <i>pic-slot</i>> <qci <i>qci</i>> <rat-type (eutran gan geran hspa others utran wlan)> <session-state></pre>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Display the status information, such as the number of subscribers, active sessions, and so on, for one or more Serving Gateways (S-GWs). If a gateway name is not specified, then the status information for all the S-GWs is displayed.
Options	<p>none—(Same as brief) Display the gateway status information in brief.</p> <p>brief detail —(Optional) Display the specified level of output.</p> <p>fpc-slot <i>fpc-slot</i>—(Optional) Display the status information for the specified FPC slot number.</p> <p>gateway <i>gateway</i>—(Optional) Display the status information for the specified gateway name.</p> <p>gtpv2-priority-level <i>gtpv2-priority-level</i>—(Optional) Display the status information for the GTPv2 priority specified. You can specify a priority of 1 through 15.</p> <p>pic-slot <i>pic-slot</i>—(Optional) Display the status information for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.</p> <p>qci <i>qci</i>—(Optional) Display the status information for the specified QoS Class Identifier (QCI).</p> <p>rat-type (eutran gan geran hspa others utran wlan)—(Optional) Display the status information for the specified Radio Access Technology (RAT).</p> <p>session-state—(Optional) Display the session state of subscriber sessions anchored on one or more S-GWs.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show unified-edge sgw status preemption-list on page 1180
List of Sample Output	<p>show unified-edge sgw status brief on page 1297</p> <p>show unified-edge sgw status detail on page 1298</p>

[show unified-edge sgw status session-state on page 1298](#)

Output Fields [Table 116 on page 1296](#) lists the output fields for the **show unified-edge sgw status** command. Output fields are listed in the approximate order in which they appear.

Table 116: show unified-edge sgw status Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the S-GW.	All levels
Mobile gateway status		
FPC SLOT	FPC slot number of the interface for which the status information is displayed.	detail
PIC SLOT	PIC slot number of the FPC for which the status information is displayed.	detail
State	State of the services PIC on the S-GW: <ul style="list-style-type: none"> • Standalone • Active—Services PIC is an active member. • Backup—Services PIC is a backup. 	detail
Active Subscribers	Number of active subscribers on the gateway.	All levels
Active Sessions	Number of active sessions on the gateway.	All levels
Active Bearers	Number of bearers in Active state.	All levels
Idle Subscribers	Number of idle subscribers on the gateway.	All levels
Idle Sessions	Number of idle sessions on the gateway.	All levels
Idle Bearers	Number of idle bearers on the gateway.	All levels
Suspended Subscribers	Number of suspended subscribers on the gateway.	All levels
Suspended Sessions	Number of suspended sessions on the gateway.	All levels
Suspended Bearers	Number of suspended bearers on the gateway.	All levels
Indirect Tunnels	Number of indirect tunnels created during handover procedures.	All levels
CPU Load (%)	Percentage of the CPU load.	All levels
Memory Load (%)	Percentage of the memory load.	All levels

State

The following information about the session state is displayed:

Table 116: show unified-edge sgw status Output Fields (*continued*)

Field Name	Field Description	Level of Output
Initial	Number of sessions being initialized.	session-state
Default bearer setup wait	Number of sessions waiting for the default bearer to be set up.	session-state
Sync wait	Number of sessions waiting for the synchronization to the backup services PIC.	session-state
Established	Number of sessions established.	session-state
Cleaning up	Number of sessions being cleaned up.	session-state
Idle mode	Number of sessions in idle mode.	session-state
Suspended	Number of suspended sessions.	session-state
PFE wait	Number of sessions waiting for a response from the Packet Forwarding Engine.	session-state
PGW wait	Number of sessions waiting for a response from the Packet Data Network Gateway (P-GW) during handovers.	session-state
MME wait	Number of sessions waiting for a request from the Mobility Management Entity (MME) during handovers.	session-state

Sample Output

```

show unified-edge sgw status brief  user@host> show unified-edge sgw status brief
                                     Gateway: SGW
                                     Mobile gateway status :
                                     Active Subscribers    :           1
                                     Active Sessions       :           1
                                     Active Bearers        :           1
                                     Idle Subscribers      :           0
                                     Idle Sessions         :           0
                                     Suspended Subscribers :           0
                                     Suspended Sessions    :           0
                                     Indirect Tunnels      :           0
                                     Idle Bearers          :           0
                                     Suspended Bearers     :           0
                                     CPU Load (%)         :           0
                                     Memory Load (%)       :          34
                                     Gateway: SGW2
                                     Mobile gateway status :
                                     Active Subscribers    :           0
                                     Active Sessions       :           0
                                     Active Bearers        :           0
                                     Idle Subscribers      :           0
                                     Idle Sessions         :           0
                                     Suspended Subscribers :           0
                                     Suspended Sessions    :           0
                                     Indirect Tunnels      :           0

```

```
Idle Bearers           :           0
Suspended Bearers      :           0
CPU Load (%)           :           0
Memory Load (%)        :           34
```

```
show unified-edge sgw status detail  user@host> show unified-edge sgw status detail
status detail                        Gateway: SGW
                                     Mobile gateway status:

                                     FPC SLOT: 1 PIC SLOT: 0
                                     State              : Standalone
                                     Active Subscribers  : 1
                                     Active Sessions     : 1
                                     Active Bearers      : 1
                                     Idle Subscribers    : 0
                                     Idle Sessions       : 0
                                     Suspended Subscribers : 0
                                     Suspended Sessions   : 0
                                     Indirect Tunnels     : 0
                                     Idle Bearers        : 0
                                     Suspended Bearers    : 0
                                     CPU Load (%)         : 0
                                     Memory Load (%)      : 34
Gateway: SGW2
                                     Mobile gateway status:

                                     FPC SLOT: 3 PIC SLOT: 1
                                     State              : Standalone
                                     Active Subscribers  : 0
                                     Active Sessions     : 0
                                     Active Bearers      : 0
                                     Idle Subscribers    : 0
                                     Idle Sessions       : 0
                                     Suspended Subscribers : 0
                                     Suspended Sessions   : 0
                                     Indirect Tunnels     : 0
                                     Idle Bearers        : 0
                                     Suspended Bearers    : 0
                                     CPU Load (%)         : 0
                                     Memory Load (%)      : 34
```

```
show unified-edge sgw status session-state  user@host> show unified-edge sgw session-state
status session-state                    Gateway: SGW
                                     Mobile gateway status:
                                     State:
                                     Initial              : 0
                                     Default bearer setup wait : 0
                                     Sync wait            : 0
                                     Established           : 1
                                     Cleaning up          : 1
                                     Idle mode            : 0
                                     Suspended            : 0
                                     PFE wait            : 0
                                     PGW wait            : 0
                                     MME wait            : 0
Gateway: SGW2
                                     Mobile gateway status:
                                     State:
```


Initial	:	0
Default bearer setup wait	:	0
Sync wait	:	0
Established	:	0
Cleaning up	:	0
Idle mode	:	0
Suspended	:	0
PFE wait	:	0
PGW wait	:	0
MME wait	:	0

show unified-edge sgw subscribers

Syntax	show unified-edge sgw subscribers <brief extensive> <fpc-slot <i>fpc-slot</i>> <gateway <i>gateway</i>> <gtpv2-priority-level <i>gtpv2-priority-level</i>> <imsi <i>imsi</i>> <msisdn <i>msisdn</i>> <peer <i>peer</i>> <pic-slot <i>pic-slot</i>> <qci <i>qci</i>>
Release Information	Command introduced in Junos OS Mobility Release 11.4W.
Description	Display the subscriber information for one or more Serving Gateways (S-GWs). If a gateway name is not specified, then the subscriber information for all the S-GWs is displayed.
Options	<p>none—(Same as brief) Display the subscriber information in brief.</p> <p>brief extensive —(Optional) Display the specified level of output.</p> <p>fpc-slot <i>fpc-slot</i>—(Optional) Display the subscriber information for the specified FPC slot number.</p> <p>gateway <i>gateway</i>—(Optional) Display the subscriber information for the specified gateway name.</p> <p>gtpv2-priority-level <i>gtpv2-priority-level</i>—(Optional) Display the subscriber information for the GTPv2 priority specified. You can specify a priority of 1 through 15.</p> <p>imsi <i>imsi</i>—(Optional) Display the subscriber information for the specified International Mobile Subscriber Identity (IMSI).</p> <p>msisdn <i>msisdn</i>—(Optional) Display the subscriber information for the specified Mobile Station ISDN (MSISDN) number.</p> <p>peer <i>peer</i>—(Optional) Display the subscriber information for the specified peer IP address.</p> <p>pic-slot <i>pic-slot</i>—(Optional) Display the subscriber information for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.</p> <p>qci <i>qci</i>—(Optional) Display the subscriber information for the specified QoS Class Identifier (QCI).</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• clear unified-edge sgw subscribers on page 1272

List of Sample Output [show unified-edge sgw subscribers brief on page 1305](#)
[show unified-edge sgw subscribers extensive on page 1306](#)

Output Fields [Table 117 on page 1301](#) lists the output fields for the **show unified-edge sgw subscribers** command. Output fields are listed in the approximate order in which they appear.

Table 117: show unified-edge sgw subscribers Output Fields

Field Name	Field Description	Level of Output
Gateway	Name of the S-GW.	All levels
IMSI	IMSI of the subscriber's user equipment.	brief
MSISDN	MSISDN number of the subscriber's user equipment.	brief
ACS Peer Ctrl Address	Control plane IP address of the access peer.	brief
S5 Peer Ctrl Address	Control plane IP address of the peer on the S5 interface.	brief
APN	Access point name (APN) to which the subscriber is attached.	brief
Subscriber Information:		
UE:		
IMSI	IMSI of the subscriber's user equipment.	extensive
IMEI	International Mobile Station Equipment Identity (IMEI) of the subscriber's user equipment.	extensive
MSISDN	MSISDN number of the subscriber's user equipment.	extensive
MS-Timezone	Time zone to which the subscriber's Mobile Station (MS) or user equipment belongs.	extensive
(DST)	Daylight saving time applicable within the time zone.	extensive
User Location Info:		
MCC	Mobile country code (MCC) of the subscriber.	extensive
MNC	Mobile network code (MNC) of the subscriber.	extensive
LAC	Location area code (LAC) of the subscriber.	extensive
CI	Cell Identity (CI) of the subscriber.	extensive
SAC	Service area code (SAC) of the subscriber.	extensive
RAC	Routing area code (RAC) of the subscriber.	extensive

Table 117: show unified-edge sgw subscribers Output Fields (*continued*)

Field Name	Field Description	Level of Output
TAC	Tracking area code (TAC) of the subscriber.	extensive
ECI	E-UTRAN Cell identifier (ECI) of the subscriber.	extensive
RAT Type	Type of Radio Access Technology (RAT) used.	extensive
SGW Control IP	Control plane IP address of the S-GW on the S11 or S4 interfaces.	
SGW Control TEID	Control plane Tunnel Endpoint Identifier (TEID) of the S-GW on the S11 or S4 interfaces.	extensive
MME Control IP	Control plane IP address of the Mobility Management Entity (MME) on the S11 interface.	extensive
MME Control TEID	Control plane TEID of the MME on the S11 interface.	extensive
SGSN Control IP	Control plane IP address of the Serving GPRS Support Node (SGSN) on the S4 interface.	extensive
SGSN Control TEID	Control plane TEID of the SGSN on the S4 interface.	extensive
ISR	Idle mode signaling reduction (enabled or disabled). If this is enabled, then both the MME and SGSN information is displayed in the command output. If it is disabled, then the either the MME or SGSN information is displayed.	extensive
Active Peer	Indicates whether the MME or the SGSN is actively sending control messages to S-GW.	extensive
Serving Network	The following information about the network serving the subscriber is displayed: <ul style="list-style-type: none"> • MCC—Mobile country code of the network. • MNC—Mobile network code of the network. 	extensive
State	State of the subscriber: idle, active, or suspended.	extensive

PDN session information:

PDN Session:

APN name	Access point name for the Packet Data Network (PDN) session.	extensive
V4 Addr	IPv4 address of the subscriber.	extensive
V6 Addr	IPv6 address of the subscriber.	extensive
Direct Tunnel	Status of the GTPv1 direct tunnel: enabled or disabled.	extensive
Up time	Time (in <i>hh:mm:ss</i> [hours:minutes:seconds] format) for which the PDN session has been up.	extensive

Table 117: show unified-edge sgw subscribers Output Fields (*continued*)

Field Name	Field Description	Level of Output
SGW S5 C IP	IP address of the S5 GTP-C tunnel on the S-GW side to which the PDN Gateway (P-GW) will send control messages for the subscriber.	extensive
PGW S5 C IP	IP address of the S5 GTP-C tunnel on the P-GW side to which the S-GW will send control messages for the subscriber.	extensive
SGW S5 C TEID	TEID of the S5 GTP-C tunnel on the S-GW side. The P-GW sends this TEID in the GTP header in all control messages to the S-GW.	extensive
PGW S5 C TEID	TEID of the S5 GTP-C tunnel on the P-GW side. The S-GW sends this TEID in the GTP header in all control messages to the P-GW.	extensive
PGW CSID	Connection Set Identifier (CSID) allocated by the P-GW.	extensive
MME CSID	Connection Set Identifier (CSID) allocated by the Mobile Management Entity (MME).	extensive
Addr scheme	Addressing scheme used for IP address allocation.	extensive
Selection mode	Selection mode configured for the APN on the P-GW.	extensive
SPIC	FPC and PIC slots for the services PIC on which the subscriber control session is anchored.	extensive
APFE	FPC and PIC slots for the anchor Packet Forwarding Engine for the PDP session.	extensive
State	State of the subscriber session on the signaling plane.	extensive
APN AMBR	The aggregate maximum bit rate (AMBR) negotiated for the PDP session is displayed for the following: <ul style="list-style-type: none"> AMBR-DL—Negotiated AMBR in the downlink direction. AMBR-UL—Negotiated AMBR in the uplink direction. 	extensive
Bearer:		
NSAPI/EBI	Network Service Access Point Identifier (NSAPI) or the Evolved Packed System Bearer ID (EBI) for the session.	extensive
SGW ACS IP	Data plane IP address of the S-GW on the S1u, S4, or S12 interface.	
ACS PEER IP	Remote data plane IP address of the peer on the S1u, S4, or S12 interface.	extensive
SGW ACS TEID	Data plane TEID of the S-GW on the S1u, S4, or S12 interface.	extensive
ACS PEER TEID	Remote data plane TEID of the peer on the S1u, S4, or S12 interface.	extensive
SGW S5 U IP	IP address of the S-GW to which the P-GW sends the data packets for the bearer.	extensive

Table 117: show unified-edge sgw subscribers Output Fields (*continued*)

Field Name	Field Description	Level of Output
PGW S5 U IP	IP address of the P-GW to which the S-GW sends the data packets for the bearer.	extensive
SGW S5 U TEID	Data TEID allocated by the S-GW that identifies the data tunneling endpoint for all data packets coming in from the data peer. This is sent in the GTP header for all the data packets sent from the S-GW to the P-GW.	extensive
PGW S5 U TEID	Data TEID allocated by the P-GW that identifies the data tunneling endpoint for all data packets coming in from the data peer. This is sent in the GTP header for all the data packets sent from the P-GW to the S-GW.	extensive
Charging ID	Charging ID for the session. The charging ID is the unique bearer identity sent in accounting messages and in Charging Data Records (CDRs).	extensive
State	Represents the state of the subscriber in the plane. This parameter is used internally by the P-GW.	extensive
Idle count	Number of times that the bearer has transitioned into idle mode for the subscriber.	extensive
Idle Timeout	<p>Idle timeout for the session, in minutes. The following information regarding the idle timeout is displayed in parentheses:</p> <ul style="list-style-type: none"> • Internal profile ID for idle timeout on the Packet Forwarding Engine. • Current timeout count that Packet Forwarding Engine reported for the subscriber. • Total timeout count that the Packet Forwarding Engine needs to report to be considered as an idle timeout for the subscriber. 	extensive
QoS Parameters	<p>The following parameters for the user equipment related to quality of service (QoS) are displayed:</p> <ul style="list-style-type: none"> • QCI—QoS Class Identifier. • ARP: (PL/PVI/PCI)—The following parameters related to ARP are displayed: <ul style="list-style-type: none"> • Priority level (PL). • Preemption Vulnerability Indicator (PVI) • Preemption Capability Indicator (PCI) • Fwd Class—Forwarding class • Loss Priority—Packet loss priority 	extensive

Table 117: show unified-edge sgw subscribers Output Fields (*continued*)

Field Name	Field Description	Level of Output
Charging information	<p>The following information related to charging is displayed:</p> <ul style="list-style-type: none"> • Profile ID—ID of the charging profile associated with the bearer. • Profile name—Name of the charging profile associated with the bearer. • State—Current charging state for the bearer. • Previous State—Previous charging state for the bearer. • Profile selection criteria—Selection source (home, visitor, roamer, and default) for the charging profile for the bearer. • Details—Current charging flag information for the bearer, which indicates what charging features are enabled. For example, Accounting enabled, offline bearer indicates that accounting and offline charging are enabled for the bearer. 	extensive
Offline charging information	<p>The following offline charging information is displayed:</p> <ul style="list-style-type: none"> • Current service data container sequence number—Sequence number of the current local service data container. • Current partial record sequence number—Sequence number of the current partial record CDR. • Number of CDRs closed—Number of closed CDRs generated. • Number of containers closed—Number of containers closed. 	extensive
Rating group information	<p>The following information related to the rating group is displayed:</p> <ul style="list-style-type: none"> • Rating group—Default rating group associated with the bearer. • Service ID—Service identifier of the rating group. • Action ID—Action identifier of the rating group. • Trigger profile—Trigger profile number associated with the rating group. • Change condition bitmask—Rating group trigger change condition bitmask. • Action-id-bitmask—Charging action ID bitmask. • Signal bitmask—Rating group trigger signal condition bitmask. • Last signal bitmask—Previous rating group trigger signal condition bitmask. • Details—Trigger flag information. • Collection time—Time when the last control plane recorded statistics for the subscriber. The following information from the statistics received from the Packet Forwarding Engine is displayed: <ul style="list-style-type: none"> • Uplink packets—Number of packets handled in the uplink direction. • Downlink packets—Number of packets handled in the downlink direction. • Uplink bytes—Number of bytes handled in the uplink direction. • Downlink bytes—Number of bytes handled in the downlink direction. 	extensive

Sample Output

```

show unified-edge sgw subscribers brief  user@host> show unified-edge sgw subscribers brief
Gateway: SGW
      IMSI           MSISDN           ACS PEER CTRL      S5 PEER CTRL      APN
                                     Address           Address

```

```

11111111123457      111111112      200.7.1.2      200.7.0.2
jnpr-bangalore_scale

```

show unified-edge sgw subscribers extensive

```
user@host> show unified-edge sgw subscribers extensive
```

```
Gateway: SGW
```

```
Subscriber information:
```

```
UE:
```

```

IMSI:      11122330000001      IMEI: -
MSISDN:    444550000001      MS-Timezone: GMT      (DST): None      User

```

```
Location info:
```

```

MCC:      234      MNC:      567
LAC: 0x0      CI: 0x0      SAC: 0x0      RAC: 0x0      TAC: 0x4321      ECI: 0x1234568

```

```

RAT Type:      E-UTRAN      Status: Visitor
SGW Control IP: 11.11.11.11      SGW Control TEID: 0x5e001000

```

```
MME Control IP: 50.50.50.1      MME Control TEID: 0x1
```

```

ISR:      Disabled      Active Peer:      MME
Serving network: MCC: 123      MNC :456
State:      ACTIVE

```

```
PDN session information:
```

```
PDN session:
```

```
APN name:      internet123.mnc456.mcc123.gprs
```

```
V4 Addr:      11.0.0.2      V6 Address:      -
```

```

Direct Tunnel: Disabled      Up time:      1:30
SGW S5 C IP: 11.11.11.11      PGW S5 C IP: 50.50.50.50
SGW S5 C TEID: 0x5e001c00      PGW S5 C TEID: 0x2
PGW CSID: 0      MME CSID: 0
Addr scheme: None      Selection mode: MS or network provided

```

```
APN, subscription verified
```

```

SPIC:      3 /0 (FPC/PIC)      APFE:      2 /0 (FPC/PIC)
State:      SgwSessionEstablished

```

```
APN AMBR :
```

```
AMBR-DL:      2000      kbps      AMBR-UL:      2000      kbps
```

```
Bearer :
```

```

NSAPI/EBI      :5
SGW ACS IP      :11.11.11.11      ACS PEER IP :50.50.50.3
SGW ACS TEID    :0xc8160401      ACS PEER TEID :0x271b
SGW S5 U IP     :11.11.11.11      PGW S5 U IP :50.50.50.50
SGW S5 U TEID   :0xc8260401      PGW S5 U TEID :0x2712

```

```

Charging ID     :0x2
State           :SgwBearerEstablished

```

```

Idle count      :3
Idle Timeout    :0 min(0 -0,0)

```

```
QoS Parameters :
```

```

QCI      :5      ARP      :1 /0 /0 (PL/PVI/PCI)
Fwd Class : None      Loss Priority : None

```

```
Charging information: Profile ID: 1      Profile name: CP1
```

```
State: Ready      Previous State: Ga
```

```
Profile selection criteria: Static default
```

```
Details: Offline bearer
```

```
Offline charging information:
```

```

Current service data container sequence number: -
Current partial record sequence number      : 4
Number of CDRs closed                      : 4
Number of containers closed                 : 5

```


Rating group information:
Rating group: 0 Service id: 0
Action ID: 0xb000401 Trigger profile: 0
Change condition bitmask: 0x0 Action-id-bitmask: 0x0
Signal bitmask: 0x0 Last signal bitmask: 0x0
Details: Bearer trigger, Offline RG
Collection time: Thu Jan 1 01:41:45 1970
Uplink packets: 14 Downlink packets : 18
Uplink bytes: 1400 Downlink bytes : 1800

show unified-edge sgw subscribers charging

Syntax `show unified-edge sgw subscribers charging gateway gateway`
`<brief | detail | extensive>`
`<charging-profile charging-profile>`
`<fpc-slot fpc-slot>`
`<pic-slot pic-slot>`
`<transport-profile transport-profile>`

Release Information Command introduced in Junos OS Mobility Release 11.4W.

Description Display the subscribers matching the specified charging profile or transport profile on the specified Serving Gateway (S-GW).

Options `gateway gateway`—Display the subscriber information for the specified gateway name.

`brief | detail | extensive` —(Optional) Display the specified level of output.

`charging-profile charging-profile`—(Optional) Display the subscribers matching the specified charging profile name.



NOTE: You must specify either a charging profile or a transport profile to execute this command.

`fpc-slot fpc-slot`—(Optional) Display the subscriber information for the specified FPC slot number.

`pic-slot pic-slot`—(Optional) Display the subscriber information for the specified PIC slot number. You must first specify an FPC slot number before specifying the PIC slot number.

`transport-profile transport-profile`—(Optional) Display the subscribers matching the specified transport profile name.



NOTE: You must specify either a charging profile or a transport profile to execute this command.

Required Privilege Level view

Related Documentation

- [clear unified-edge sgw subscribers charging on page 1273](#)
- [show unified-edge sgw subscribers on page 1300](#)

List of Sample Output [show unified-edge sgw subscribers charging gateway SGW charging-profile cp1 brief on page 1309](#)

[show unified-edge sgw subscribers charging gateway SGW charging-profile cp1 detail on page 1309](#)

[show unified-edge sgw subscribers charging gateway SGW charging-profile cp1 extensive on page 1310](#)

Output Fields Refer to the output fields for the [show unified-edge sgw subscribers](#) command, which is the same as the output fields for the [show unified-edge sgw subscribers charging](#) command.

Sample Output

```

show unified-edge sgw subscribers charging gateway SGW charging-profile cp1 brief
user@host> show unified-edge sgw subscribers charging gateway SGW charging-profile cp1 brief
              IMSI              MSISDN              ACS PEER CTRL              S5 PEER CTRL              APN
              Address              Address
123213213123568              1926738057              79.1.1.3              114.11.11.2 internet123

show unified-edge sgw subscribers charging gateway SGW charging-profile cp1 detail
user@host> show unified-edge sgw subscribers charging gateway SGW charging-profile cp1 detail
Subscriber information:
  UE:
    IMSI:              123213213123568              IMEI: 1122334455667791
    MSISDN:              1926738057              MS-Timezone: GMT              (DST): None              User
  Location info:
    MCC:              300              MNC:              400
    LAC: 0x3e8              CI: 0xc8              SAC: 0x0              RAC: 0x0              TAC: 0x0              ECI: 0x0
    RAT Type:              E-UTRAN              Status: Visitor
    SGW Control IP: 11.11.11.11              SGW Control TEID: 0xd001000
    MME Control IP: 79.1.1.3              MME Control TEID: 0x103
    ISR:              Disabled              Active Peer:              MME
    Serving network: MCC: 123              MNC :567
    State: ACTIVE
  PDN session information:
  PDN session:
    APN name:              internet123.mnc567.mcc123.gprs
    V4 Addr:              16.16.4.6              V6 Address: -
    Direct Tunnel: Disabled              Up time:              8:16:28
    SGW S5 C IP: 11.11.11.11              PGW S5 C IP: 114.11.11.2
    SGW S5 C TEID: 0xd001c00              PGW S5 C TEID: 0x3ee
    PGW CSID: 100              MME CSID: 0
    Addr scheme: None              Selection mode: MS or network provided
  APN, subscription verified
    SPIC:              5 /0 (FPC/PIC)              APFE:              1 /0 (FPC/PIC)
    State:              SgwSessionEstablished
  APN AMBR :
    AMBR-DL: 22              kbps              AMBR-UL: 88              kbps
  Bearer :
    NSAPI/EBI :5
    SGW ACS IP :11.11.11.11              ACS PEER IP :79.1.1.3
    SGW ACS TEID :0x150400              ACS PEER TEID :0x104
    SGW S5 U IP :11.11.11.11              PGW S5 U IP :114.11.11.2
    SGW S5 U TEID :0x250400              PGW S5 U TEID :0x3ef
    Charging ID :0x3ef
    State :SgwBearerEstablished
    Idle count :0
    Idle Timeout :0 min(0 -0,0)
  QoS Parameters :

```

```

QCI          :5                      ARP          :1 /0 /0   (PL/PVI/PCI)
Fwd Class    :af2                    Loss Priority :high
Charging information: Profile ID: 1   Profile name: p_juniper
State: Ready                               Previous State: Ga
Details: Offline bearer
Rating group information:
Rating group: 0 Service id: 0
Details: Bearer trigger, Offline RG

```

```

show unified-edge sgw subscribers charging gateway SGW charging-profile cp1
subscribers charging extensive
gateway SGW
charging-profile cp1
extensive
user@host> show unified-edge sgw subscribers charging gateway SGW charging-profile cp1
extensive
Gateway: SGW
Subscriber information:
UE:
  IMSI:      111222330000001      IMEI: -
  MSISDN:    444550000001      MS-Timezone: GMT      (DST): None      User
Location info:
  MCC:      234      MNC:      567
  LAC: 0x0      CI: 0x0      SAC: 0x0      RAC: 0x0      TAC: 0x4321      ECI: 0x1234568
  RAT Type:      E-UTRAN      Status: Visitor
  SGW Control IP: 11.11.11.11      SGW Control TEID: 0x5e001000
  MME Control IP: 50.50.50.1      MME Control TEID: 0x1
  ISR:      Disabled      Active Peer:      MME
  Serving network: MCC: 123      MNC :456
  State:      ACTIVE
PDN session information:
PDN session:
  APN name:      internet123.mnc456.mcc123.gprs
  V4 Addr:      11.0.0.2      V6 Address: -
  Direct Tunnel: Disabled      Up time:      1:30
  SGW S5 C IP:  11.11.11.11      PGW S5 C IP:  50.50.50.50
  SGW S5 C TEID: 0x5e001c00      PGW S5 C TEID: 0x2
  PGW CSID:      0      MME CSID:      0
  Addr scheme: None      Selection mode: MS or network provided
APN, subscription verified
  SPIC:      3 /0 (FPC/PIC)      APFE:      2 /0 (FPC/PIC)
  State:      SgwSessionEstablished
APN AMBR :
  AMBR-DL:      2000      kbps      AMBR-UL:      2000      kbps
Bearer      :
  NSAPI/EBI      :5
  SGW ACS IP      :11.11.11.11      ACS PEER IP      :50.50.50.3
  SGW ACS TEID    :0xc8160401      ACS PEER TEID    :0x271b
  SGW S5 U IP     :11.11.11.11      PGW S5 U IP      :50.50.50.50
  SGW S5 U TEID   :0xc8260401      PGW S5 U TEID    :0x2712
  Charging ID     :0x2
  State           :SgwBearerEstablished
  Idle count      :3
  Idle Timeout    :0      min(0      -0,0)
QoS Parameters :
  QCI          :5                      ARP          :1 /0 /0   (PL/PVI/PCI)
  Fwd Class     : None                    Loss Priority : None
  Charging information: Profile ID: 1   Profile name: CP1
  State: Ready                               Previous State: Ga

```

```
Profile selection criteria: Static default
Details: Offline bearer
Offline charging information:
  Current service data container sequence number: -
  Current partial record sequence number         : 4
  Number of CDRs closed                         : 4
  Number of containers closed                    : 5
Rating group information:
  Rating group: 0 Service id: 0
  Action ID: 0xb000401                      Trigger profile: 0
  Change condition bitmask: 0x0              Action-id-bitmask: 0x0
  Signal bitmask: 0x0                        Last signal bitmask: 0x0
Details: Bearer trigger, Offline RG
  Collection time: Thu Jan  1 01:41:45 1970
  Uplink packets: 14                          Downlink packets : 18
  Uplink bytes: 1400                          Downlink bytes : 1800
```


PART 13

Index

- [Index on page 1315](#)
- [Index of Statements and Commands on page 1337](#)

Index

Symbols

#, comments in configuration statements.....	xl
(), in syntax descriptions.....	xl
3G networks	
broadband gateway.....	39
GGSN.....	49
< >, in syntax descriptions.....	xxxix
[], in configuration statements.....	xl
{ }, in configuration statements.....	xl
(pipe), in syntax descriptions.....	xl

A

AAA	
AAA profile configuration example.....	200
configuration example.....	192
configuration overview.....	148
configuration steps.....	179
configuring RADIUS servers.....	179
network element group configuration	
example.....	200
network elements.....	151
network elements configuration example.....	199
RADIUS configuration example.....	195
scalability and redundancy features.....	150
server failover.....	151
verifying the configuration.....	203
AAA profile.....	149
accounting options.....	185
applying to an APN.....	190
authentication options.....	184
configuration example.....	200
configuration steps.....	184
excluding or ignoring RADIUS attributes.....	186
overview.....	153
RADIUS options.....	154, 190
aaa statement.....	586
APN.....	677
AAA troubleshooting.....	463
aaa-override statement	
APN.....	678

aaa-profile statement	
APN.....	679
aaa-radius statement.....	604
access point name.....	412
access point name delete	412
access point name modify.....	398
Access-Accept messages.....	159
Access-Request messages.....	155
accounting	
AAA profile options.....	153, 185
network element groups.....	152, 183
overview.....	149
Accounting On messages.....	175
Accounting Start messages.....	162
accounting statement	
unified-edge profile.....	588
Accounting Stop messages.....	171
accounting-port statement.....	589
accounting-secret statement.....	589
activate maintenance mode.....	399
address assignment	
APN configuration.....	115
by the AAA server.....	191, 192
configuring AAA server override.....	191
address statement.....	590
address-assignment statement	
APN.....	680
MobileNext Broadband Gateway.....	618
ageing-window statement	
mobile pools.....	619
aggregate maximum bit rate See AMBR	
aggregated-maximum-bit-rate statement	
cos-cac.....	855
algorithm statement.....	590
allocation and retention priority See ARP	
allocation and retention-priority statement	
cos-cac.....	856
allow-dynamic-requests statement.....	591
allow-network-behind-mobile statement.....	681
allow-static-ip-address statement	
APN.....	682
AMBR	
configuring	
downlink.....	336, 340
uplink.....	337, 341
overview.....	314, 317
anchor interface DPCs and MPCs	
exceptions.....	88

anchor session DPCs	
exceptions.....	88
anchor-pfe-default-bearers-percentage statement	
Serving Gateway.....	857
anchor-pfe-guaranteed-bandwidth statement	
Serving Gateway.....	858
anchor-pfe-ipv4-nbm-prefixes statement.....	683
anchor-pfe-ipv6-nbm-prefixes statement.....	684
anchor-pfe-maximum-bearers statement	
Serving Gateway.....	859
anchor-pfes statement.....	645
anchor-service-pics statement.....	646
anchor-spics statement.....	646
anchoring-options statement.....	647
anchors	
broadband gateway.....	69, 80
configuring on broadband gateway.....	71
anonymous users	
APN configuration.....	114
anonymous-user statement	
APN.....	685
apfe-group-set statement.....	648
APN	
configuration example.....	126
HTTP header enrichment.....	134, 135, 138
network behind mobile.....	131, 133
apn-data-type statement	
APN.....	686
apn-name statement	
service selection profiles.....	754
apn-services statement.....	687
apn-type statement	
APN.....	690
APNs	
AAA configuration example.....	202
applying an AAA profile.....	190
broadband gateway.....	105, 120, 122
configuring address assignment.....	113, 115, 191
configuring anonymous users.....	114
configuring charging profiles.....	119
configuring general APN parameters.....	109
configuring QoS local policy profiles.....	119
configuring service selection.....	123
mobile network.....	46
apns statement.....	691
APN services.....	691
architecture	
3G networks.....	39

ARP.....	314
in 3G networks.....	314
in 4G networks.....	314
overview.....	314
See also preemption	
attributes statement.....	592
AuC	
mobile network.....	50
authentication	
AAA profile options.....	153, 184
overview.....	148
authentication statement.....	593
authentication-port statement.....	593
B	
background traffic class	
configuring.....	334
description.....	311
bandwidth pools.....	315
allocating for conversational traffic class.....	325
allocating for streaming traffic class.....	325
configuring.....	325
APN level.....	316
downlink.....	344
system level.....	316, 344
uplink.....	344
See also overview	
bandwidth-pool statement	
cos-cac.....	860
bearer load	
configuring	
in 3G networks.....	329
in 3G/4G networks.....	331
in 4G networks.....	327
bearer-load statement	
cos-cac.....	861
bearers	
configuring maximum number	
APN level.....	324
system level.....	324
initial QoS level.....	310
managing load.....	316
maximum number, at system or APN	
level.....	316
mobile network.....	47
preempting.....	316

- rejecting based on
 - AMBR.....337, 341
 - maximum traffic class.....317
 - upgrading based on
 - AMBR.....337, 341
 - ARP.....337
 - QCI.....336
 - bind-interface statement
 - dhcp.....629
 - block-visitors statement
 - APN.....693
 - braces, in configuration statements.....xl
 - brackets
 - angle, in syntax descriptions.....xxxix
 - square, in configuration statements.....xl
 - broadband gateway
 - 3G networks.....39
 - address assignment configuration.....115
 - anchors.....69, 80
 - and GGSN.....10
 - and IPv6 protocol.....93
 - anonymous user configuration.....114
 - APN charging profiles configuration.....119
 - APN configuration.....105, 109
 - APN configuration example.....126
 - APN QoS local policy profiles
 - configuration.....119
 - APN service selection configuration.....123
 - APNs configuration.....120, 122
 - chassis configuration.....62
 - chassis configuration example.....67
 - collocated P-GW and S-GW.....26
 - configuring anchors71
 - configuring call rate statistics.....13
 - configuring charging.....280
 - configuring fragment reassembly.....90
 - configuring gateways.....11, 30
 - configuring HPLMNs.....11, 30
 - configuring idle-mode buffering.....30
 - configuring local policies.....12
 - configuring maximum bearers.....30
 - configuring preemption.....30
 - configuring profiles.....32
 - configuring QoS.....384
 - configuring S-GW global charging
 - profiles.....282
 - control packet flow.....6
 - downlink payload packet flow.....9
 - exceptions.....88, 89
 - exceptions configuration example.....99
 - functions.....55
 - general gateway.....15
 - HTTP header enrichment.....134, 135, 138
 - interface DPC or MPC configuration.....66
 - interface redundancy.....76
 - interfaces configuration example.....67
 - interfaces redundancy configuration
 - example.....82
 - IP fragments.....90
 - IPv6 protocol.....92
 - mobile interface configuration.....120, 122
 - mobile options.....17
 - network behind mobile.....130
 - P-GW.....10, 26, 28, 29
 - physical interface overview.....63
 - QoS configuration example.....348
 - redundancy configuration.....74
 - redundancy configuration example.....82
 - restriction value configuration.....113
 - Routing Engine redundancy.....74
 - S-GW.....21, 26, 28, 29
 - S-GW user packet flow.....25
 - S1 interface.....53
 - service and tracking areas.....54
 - session DPC configuration.....64
 - session DPC configuration example.....67
 - session DPC overview.....63
 - session DPC redundancy.....75
 - session DPC redundancy configuration
 - example.....82
 - system architecture.....4
 - traceoptions.....33, 95, 97, 262, 284, 287
 - uplink payload packet flow.....7
 - user-session routing.....107
 - VRF configuration.....122
 - Broadband Gateway
 - AAA configuration.....148
 - configuring
 - QoS, overview.....323
 - GGSN.....49
 - resource manager.....19
- ## C
- CAC
 - bandwidth pools.....315
 - enforcing.....315
 - maximum bearers.....316
 - overview.....315

preemption, enabling.....	326
resource thresholds.....	316
call admission control See CAC	
call admission control troubleshooting.....	461
call detail record profile change.....	407
call rate statistics	
configuring on broadband gateway.....	13
monitoring.....	14
call-rate-statistics statement.....	981
CDR profiles	
configuring.....	298
cdr-aggregation-limit statement.....	769
cdr-profile statement.....	770
cdr-profiles statement.....	772
cdr-release statement	
charging gateways.....	773
CDRs	
GTP Prime properties.....	289
cdrs-per-file statement.....	774
Change of Authorization (CoA) Messages.....	177
charging	
configuring.....	279
configuring on broadband gateway.....	280
configuring S-GW global profiles.....	282
configuring S-GW selection order.....	282
disabling persistent storage.....	1120
enabling persistent storage.....	1119
S-GW local persistent storage	
traceoptions.....	287
S-GW traceoptions.....	284
charging configurations	
managing.....	304
monitoring.....	304
charging gateway statistics.....	434
charging profile change.....	402, 413
charging profile delete.....	406
charging profiles	
APN	
configuring.....	301
APN configuration.....	119
CDR profiles.....	298
configuring.....	300
transport profiles.....	295
trigger profiles.....	296
charging statement.....	775
APN.....	695
charging-characteristics statement	
service selection profiles.....	755
charging-gateways statement.....	779
charging-profiles statement.....	780
chassis	
broadband gateway.....	62
configuration example.....	67
monitoring.....	72
redundancy configuration.....	76, 78
chassis configuration example	
broadband gateway.....	67
class-of-service statement.....	864
classifier profiles	
configuring	
3G networks.....	333
4G networks.....	332
for 3G and 4G networks.....	334
classifier-profile statement	
local-policies.....	862
classifier-profiles statement	
cos-cac.....	863
clear unified-edge ggsn-pgw aaa radius statistics	
command.....	1018
clear unified-edge ggsn-pgw aaa statistics	
command.....	1019
clear unified-edge ggsn-pgw address-assignment	
pool command.....	1020
clear unified-edge ggsn-pgw address-assignment	
statistics command.....	1021
clear unified-edge ggsn-pgw charging cdr	
command.....	1110
clear unified-edge ggsn-pgw charging cdr wfa	
command.....	1111
clear unified-edge ggsn-pgw charging	
local-persistent-storage statistics	
command.....	1112
clear unified-edge ggsn-pgw charging path	
statistics command.....	1113
clear unified-edge ggsn-pgw charging transfer	
statistics command.....	1114
clear unified-edge ggsn-pgw gtp peer statistics	
command.....	1194
clear unified-edge ggsn-pgw gtp statistics	
command.....	1196
clear unified-edge ggsn-pgw ip-reassembly	
statistics command.....	1184
clear unified-edge ggsn-pgw statistics	
command.....	1074
clear unified-edge ggsn-pgw subscribers charging	
command.....	1077
clear unified-edge ggsn-pgw subscribers	
command.....	1075

clear unified-edge ggsn-pgw subscribers peer command.....	1078	S12 interface.....	254
clear unified-edge sgw charging cdr command.....	1115	S4 interface.....	257
clear unified-edge sgw charging local-persistent-storage statistics command.....	1116	configuring address assignment APN configuration.....	115
clear unified-edge sgw charging path statistics command.....	1117	configuring anonymous users APN configuration.....	114
clear unified-edge sgw charging transfer statistics command.....	1118	configuring APNs gateways configuration.....	11
clear unified-edge sgw gtp peer statistics command.....	1197	configuring broadband gateway APN configuration.....	105, 109
clear unified-edge sgw gtp statistics command.....	1198	configuring call rate statistics gateways configuration.....	13
clear unified-edge sgw idle-mode-buffering statistics command.....	1270	configuring charging profiles APNs.....	119
clear unified-edge sgw ip-reassembly statistics command.....	1185	configuring chassis interfaces for mobility redundancy.....	78
clear unified-edge sgw statistics command.....	1271	session DPC redundancy.....	76
clear unified-edge sgw subscribers charging command.....	1273	configuring HPLMNs gateways.....	11, 30
clear unified-edge sgw subscribers command.....	1272	configuring idle-mode buffering gateways.....	30
clear unified-edge sgw subscribers peer command.....	1274	configuring interface DPCs or MPCs user traffic.....	66
client statement resource management.....	1000	configuring interfaces for mobility redundancy.....	78
collocated P-GW configuration.....	525	configuring local policies gateways.....	12
S-GW configuration.....	525	configuring maximum bearers gateways.....	30
collocated gateways P-GW and S-GW.....	28, 29	configuring mobile interfaces mobility.....	120, 122
comments, in configuration statements.....	xl	configuring PFEs anchor configuration.....	71
configuration broadband gateway.....	62	configuring preemption gateways.....	30
broadband gateway interface PFEs.....	74	configuring QoS local policy profiles APNs.....	119
broadband gateway services PICs.....	74	configuring redundancy interfaces for mobility.....	78
configuration example APN.....	126	session DPC.....	76
chassis.....	67	configuring restriction value APN configuration.....	113
exceptions.....	99	configuring S-GW charging configuration.....	280, 282
for QoS.....	348	gateways configuration.....	30
redundancy.....	82	profile configuration.....	32
configuring GTP parameters.....	249, 259, 261	QoS configuration.....	384
S1-U interface.....	256	configuring service selection APNs.....	123
S11 interface.....	252		

configuring session DPC		
control messages.....	64	
redundancy.....	76	
configuring session DPCs		
anchor configuration.....	71	
connection set identifiers.....	224	
container-limit statement.....	781	
control messages		
session DPC configuration.....	64	
control packet flow		
broadband gateway.....	6	
control plane		
configuring GTP services		
for GGSN/P-GW.....	230	
control statement		
GTP.....	917	
Gn.....	918	
Gp.....	918	
S4.....	918	
S5.....	918	
S8.....	918	
peer group.....	919	
conventions		
text and syntax.....	xxxix	
conversational traffic class		
configuring.....	334	
description.....	311	
CoS policy profile		
AMBR in.....	317	
configuring		
in 3G networks.....	338	
in 3G/4G networks.....	340	
in 4G networks.....	336	
GBR in.....	318	
maximum QCI in.....	317	
maximum traffic class in.....	317	
MBR in.....	318	
overview.....	317	
policer actions.....	318	
cos-cac statement.....	865	
cos-policy-profile statement		
local-policies.....	867	
cos-policy-profiles statement		
cos-cac.....	868	
count statement		
HTTP header enrichment.....	694	
CPU		
managing load	316	
CPU load		
configuring		
in 3G networks.....	329	
in 3G/4G networks.....	331	
in 4G networks.....	327	
cpu statement		
cos-cac.....	869	
curly braces, in configuration statements.....	xl	
current-hop-limit statement		
IPv6 router advertisement.....	897	
customer support.....	xl	
contacting JTAC.....	xl	
D		
data plane		
configuring GTP services		
for GGSN/P-GW.....	232	
data rate statistics.....	435	
data statement		
GTP.....	920	
Gn.....	921	
Gp.....	921	
S4.....	921	
S5.....	921	
S8.....	921	
datapath		
traceoptions.....	97	
ddn-delay-sync statement.....	922	
dead server detection.....	152	
configuring.....	181	
dead-criteria-retries statement.....	594	
dead-server-retry-interval statement		
dhcp.....	630	
dead-server-successive-retry-attempt statement		
dhcp.....	631	
dedicated statement		
IPsec.....	649	
default settings		
preemption.....	323	
resource thresholds	317	
default-pool statement		
mobile pools.....	619	
default-profile statement.....	697, 782	
default-rating-group statement.....	783	
default-service-id statement.....	784	
delete access point name.....	401	
deployment		
mobile network.....	50	

- description statement
 - APN.....698
 - CDR profiles.....785
 - charging profiles.....785
 - transport profiles.....785
 - trigger profiles.....785
 - destination-address statement
 - HTTP header enrichment.....698
 - destination-address-range statement
 - HTTP header enrichment.....699
 - destination-ipv4-address statement
 - GTP Prime.....786
 - destination-port statement
 - GTP Prime.....787
 - destination-port-range statement
 - HTTP header enrichment.....699
 - destination-ports statement
 - HTTP header enrichment.....700
 - destination-prefix-list statement
 - HTTP header enrichment.....701
 - DHCP
 - AAA address override.....191
 - configuring.....208
 - APN.....209
 - dhcp-proxy-client statement
 - APN.....702
 - dhcp.....632
 - dhcp-server-selection-algorithm statement
 - dhcp.....633
 - dhcipv4-profiles statement
 - dhcp.....634
 - dhcipv4-proxy-client-profile statement
 - APN.....703
 - dhcipv6-profiles statement
 - dhcp.....635
 - dhcipv6-proxy-client-profile statement
 - APN.....704
 - dial-options statement
 - IPsec.....649
 - diffserv model
 - QoS support on broadband gateway.....310
 - direction statement
 - trigger profiles.....788
 - disable statement
 - idle mode buffering.....982
 - IPv6 router advertisement.....898
 - disable-replication statement.....789
 - Disconnect Request messages.....176
 - disk-space-policy statement.....790
 - dl-bandwidth-pool statement
 - local-policies.....870
 - dns-server statement
 - APN.....705
 - documentation
 - comments on.....xl
 - down-detect-time statement
 - GTP Prime.....791
 - downlink payload packet flow
 - broadband gateway.....9
 - DPCs
 - configuring interface DPCs.....66
 - drop-member-traffic statement
 - aggregated multiservices.....650
 - DSCP marking
 - subscriber packets.....346, 347
 - dscp-code-point statement
 - GTP.....923
 - dscp-ipv6-rewrite-rule-name statement
 - class-of-service.....870
 - dscp-ipv6-rewrite-rule-name-ingress statement
 - class-of-service.....871
 - dscp-rewrite-rule-name statement
 - class-of-service.....871
 - dscp-rewrite-rule-name-ingress statement
 - class-of-service.....872
 - dynamic requests.....150
 - enabling for a RADIUS server.....181
 - dynamic-requests-secret statement.....594
- ## E
- echo-interval statement
 - GTP.....924
 - GTP Prime.....792
 - echo-n3-requests statement
 - GTP.....926
 - echo-t3-response statement
 - GTP.....928
 - edit access address-assignment statement
 - hierarchy.....554
 - edit interfaces ams statement hierarchy.....555
 - edit interfaces apfe statement hierarchy.....556
 - edit interfaces mif statement hierarchy.....557
 - edit services hcm statement hierarchy.....558
 - edit services ip-reassembly statement
 - hierarchy.....559
 - edit services service-set statement hierarchy.....559
 - edit unified-edge gateways ggsn-pgw statement
 - hierarchy.....564

edit unified-edge gateways sgw statement		exceptions	
hierarchy.....	574	broadband gateway.....	88, 89
edit unified-edge gateways statement		configuration example.....	99
hierarchy.....	563	traceoptions.....	95
edit unified-edge mobile-options statement		exclude statement	
hierarchy.....	582	RADIUS.....	595
edit unified-edge resource-management statement		trigger profiles.....	794
hierarchy.....	582	exclude-ie-options statement.....	797
edit unified-edge statement hierarchy.....	559	exclude-pools statement	
egress rewrite rules		APN.....	707
configuring.....	345	exclude-v6pools statement	
overview		APN.....	708
overview.....	319	exit maintenance mode.....	400
egress-key statement		expire-timer statement	
aggregated multiservices.....	971	idle mode buffering.....	983
EIR		external-assigned statement	
mobile network.....	50	mobile pools.....	620
enable-reduced-partial-cdrs statement.....	793	F	
enable-rejoin statement		failover	
aggregated multiservices.....	651	broadband gateway anchors.....	80
encrypt statement		family statement	
HTTP header enrichment.....	706	aggregated multiservices.....	652
EPC		mobile interface.....	983
mobile network.....	44	mobile pools.....	621
error-indication-interval statement.....	898	file-age statement.....	801
GTP.....	930	file-creation-policy statement.....	802
errors		file-format statement.....	803
exceptions.....	89	file-name-private-extension statement.....	804
evolved packet core		file-size statement.....	805
mobile network.....	44	filter statement	
example		mobile interface.....	984
collocated P-GW configuration.....	525	font conventions.....	xxxix
collocated S-GW configuration.....	525	forwarding classes	
GTP configuration.....	265	mapping to QCI values.....	332
HTTP header enrichment.....	138	mapping to traffic classes.....	333
multigateway P-GW configuration.....	535	forwarding-class statement	
multigateway S-GW configuration.....	535	GTP.....	931
network behind mobile.....	133	forwarding-packages statement.....	985
S-GW configuration.....	519	fragment	
S-GW QoS and CAC configuration.....	385	broadband gateway handling.....	90
exceed-action policer		fragment reassembly	
configuring		configuring on broadband gateway.....	90
for GBR.....	339	from statement	
overview.....	318	HTTP header enrichment.....	709
exceed-action statement		service selection profiles.....	756
cos-cac.....	872	functions	
		S-GW.....	55

- functions in mobile network
 - APNs.....46
 - packet data network gateway.....42
- G**
- gateway configurations
 - monitoring.....14
- gateways
 - configuring on broadband gateway.....11, 30
- GBR
 - configuring in traffic classes.....339
 - overview.....312, 318
- GBR bearers.....315
 - See also bandwidth pools
- general gateway
 - traceoptions.....15
- GGSN
 - broadband gateway.....10, 49
 - functions in mobile network.....37, 40
 - in 3G networks.....49
- ggsn-pgw statement.....986
- Gi to Gn data packets trace.....446
- global-profile statement
 - Serving Gateway.....806
- Gn interface
 - configuring GTP services
 - for GGSN/P-GW.....236
- gn statement
 - GTP.....932
- Gn to Gi (GTP-U) data packet trace442
- Gp interface
 - configuring GTP services
 - for GGSN/P-GW.....238
- gp statement
 - GTP.....934
- GPRS Tunneling Protocol.....396
- group statement
 - APN.....710
- GTP
 - configuring.....249, 259, 261
 - connection set identifiers.....224
 - echo requests
 - version support for.....217
 - example.....265
 - GPRS interfaces.....215
 - overview.....216
 - path management217
 - default settings.....217
 - disabling.....247
 - echo requests.....217
 - echo-request messages.....218
 - overview.....216
 - path failure.....219
 - path success.....218
 - restart counters.....223
 - supported versions.....214
 - traceoptions.....262
 - tunnel endpoint identifiers.....225
 - tunnel management
 - create requests.....221
 - default settings.....220
 - overview.....220
 - path failure.....222
 - path success.....221, 222
 - request messages.....221
 - update/delete requests.....222
 - version support.....220
 - tunnel management functions.....220
- GTP interface address change.....395
- GTP interface delete.....396
- GTP Prime peers
 - GTP Prime properties.....290
- GTP Prime properties
 - configuring.....289, 290
- GTP redirect See user-session routing
- GTP services
 - configuring
 - 3GPP interfaces in different VRFs.....242
 - control plane for GGSN/P-GW.....230
 - data plane for GGSN/P-GW.....232
 - default settings.....227
 - GGSN.....244
 - GGSN/P-GW.....229
 - Gn interface.....236
 - Gp interface.....238
 - loopback address.....228
 - peer group.....245
 - S5 and S8 interfaces.....239, 241
 - S5 interface.....233
 - S8 interface.....235
 - trace options.....247
 - configuring on gateway
 - overview.....226
- GTP signaling.....430, 458
- gtp statement
 - GGSN.....936
 - P-GW.....936
 - Serving Gateway.....941

GTP-C messages		
route lookup.....	225	
GTP-U errors		
exceptions.....	89	
gtp statement.....	807	
guaranteed bit rate See GBR		
guaranteed-bit-rate statement		
cos-cac.....	873	
H		
hash-keys statement		
aggregated multiservices.....	972	
hcm statement		
HTTP header enrichment.....	711	
header-type statement		
GTP Prime.....	808	
high statement		
cos-cac.....	874	
high-availability-options statement		
aggregated multiservices.....	653	
history statement		
call-rate statistics.....	986	
home users		
mobile network.....	11	
home-plmn statement.....	987	
home-profile statement.....	712, 809	
HSS		
mobile network.....	50	
HTTP header enrichment		
APN.....	134, 135, 138	
example.....	138	
P-GW.....	134, 135	
I		
icons defined, notice.....	xxviii	
idle-mode-buffering statement.....	988	
idle-timeout statement		
APN.....	713	
idle-timeout-direction statement		
APN.....	714	
ignore statement.....	597	
imei statement		
service selection profiles.....	757	
imsi statement		
network behind mobile.....	715	
service selection profiles.....	758	
indirect-tunnel statement.....	945	
inet-pool statement		
APN.....	716	
inet-precedence-rewrite-rule-name statement		
class-of-service.....	874	
inet-precedence-rewrite-rule-name-ingress		
statement		
class-of-service.....	875	
inet6-pool statement		
APN.....	717	
information element (IE)		
initial QoS level.....	310	
ingress rewrite rules		
configuring.....	345	
overview		
overview.....	319	
ingress-key statement		
aggregated multiservices.....	974	
ingress-rewrite-rules statement		
class of service.....	875	
input statement		
mobile interface.....	988	
inter-mobile-traffic statement		
APN.....	718	
interactive traffic class		
configuring.....	334	
description.....	311	
interface configuration example		
broadband gateway.....	67	
interface DPC and MPC		
anchors.....	69	
interface DPCs or MPCs		
configuring for user traffic.....	66	
interface mobile interfaces		
configuring.....	120, 122	
interface redundancy configuration example		
broadband gateway.....	82	
interface statement.....	989	
anchor Packet Forwarding Engine.....	654	
GTP.....	946	
services PIC.....	656	
session PIC.....	657	
interface-service statement		
aggregated multiservices.....	975	
interfaces		
GTP.....	249, 259, 261, 265	
mobile		
applying rewrite rules.....	346, 347	
S1-U.....	256	
S11.....	252	
S12.....	254	
S4.....	257	

- interfaces for mobility
 - redundancy configuration.....78
- interfaces statement
 - aggregated multiservices.....658
 - aggregated Packet Forwarding Engine.....660
 - class-of-service.....876
 - mobile interface.....990
- Interim-Update messages.....166
- interval statement
 - call-rate statistics.....991
- IP fragments
 - broadband gateway handling.....90
- ip-reassembly statement.....899
- ip-reassembly-profile statement.....900
- IPsec services
 - adaptive services interfaces
 - IPSec security associations,
 - displaying.....1062
- ipsec-interface-id statement
 - IPsec.....661
- IPv6
 - mobile network.....52
- IPv6 protocols
 - broadband gateway parameters.....92, 93
- ipv6-router-advertisement statement.....901
- J**
 - jnxMbgPgwGtpPeerDNThresPerPeerNotif
 - trap.....460
 - jnxMbgPgwGtpPeerDownNotif trap.....459
 - jnxMbgPgwGtpPeerGWUpNotif trap.....459
 - jnxMbgPgwSMBearersThresGblNotif trap.....461
 - jnxMbgPgwSMBearersThresPerSPNotif trap.....461
 - jnxMbgPgwSMGtpEventNotif trap.....460
 - jnxMbgPgwSMSessionEstFailThresPerTCNotif
 - trap.....461
 - jnxMbgPgwSMSubscribersThresGblNotif
 - trap.....460
 - jnxMbgPgwSMSubscribersThresPerSPNotif
 - trap.....460, 461
- L**
 - lease-time statement
 - dhcp.....636
 - load-balancing-options statement
 - aggregated multiservices.....662, 976
 - IPsec.....663
 - local persistent storage
 - S-GW traceoptions.....287
 - local policies
 - configuring on broadband gateway.....12
 - specifying
 - bandwidth pools.....344
 - classifier profiles.....343
 - policy profiles.....344
 - resource thresholds.....344
 - local policies profile
 - configuring.....343
 - local policy
 - applying
 - system level.....344
 - local statement
 - APN.....719
 - local-persistent-storage-options statement.....810
 - local-policies.....877
 - local-policy-profile statement
 - APN.....720
 - Broadband Gateway.....878, 992
 - local-storage statement.....811
 - logical-system statement
 - APN.....721
 - loopback address
 - configuring for GTP services.....228
 - low statement
 - cos-cac.....879
 - LTE See networks
- M**
 - maintenance mode.....394
 - manuals
 - comments on.....xl
 - many-to-one statement
 - aggregated multiservices.....664
 - max-reassembly-pending-packets statement
 - IP reassembly.....902
 - maximum bearers
 - configuring
 - APN level.....324
 - system level.....324
 - maximum bit rate See MBR
 - maximum pending requests.....152
 - maximum QCI
 - overview.....317
 - maximum traffic class
 - overview.....317
 - maximum-advertisement-interval statement
 - IPv6 router advertisement.....903

maximum-bearers statement		mobile network	
APN.....	722	3G.....	37
Broadband Gateway.....	880, 993	4G/LTE.....	37
service selection profiles.....	759	APNs.....	46
maximum-bit-rate statement		bearers.....	47
cos-cac.....	881	broadband gateway architecture.....	4
maximum-initial-advertisement-interval statement		deployment.....	50
IPv6 router advertisement.....	904	EPC.....	44
maximum-initial-advertisements statement		functions.....	55
IPv6 router advertisement.....	905	GGSN.....	37, 40
maximum-pending-reqs-limit statement.....	597	IPv6.....	52
MBR		network behind mobile.....	130
configuring in traffic classes.....	338, 343	P-GW.....	28, 29, 37, 40, 52
overview.....	312, 318	packet data network gateway.....	42
mcc statement.....	994	S-GW.....	21, 28, 29
member-failure-options statement		S-GW user packet flow.....	25
aggregated multiservices.....	665	S1 interface.....	53
member-interface statement		service and tracking areas.....	54
aggregated multiservices.....	667	user types.....	11
memory		mobile options	
managing load	316	traceoptions.....	17
memory load		mobile options statement.....	1001
configuring		mobile subscribers	
in 3G networks.....	330	CDR profiles.....	298
in 3G/4G networks.....	332	charging profiles.....	300
in 4G networks.....	328	APN.....	301
Memory monitoring.....	433	monitoring.....	304
memory statement		persistent storage of CDR.....	291
cos-cac.....	882	tracing operations.....	302
mif statement		transport profiles.....	295
class of service.....	883	trigger profiles.....	296
minimum-advertisement-interval statement		mobile-interface statement	
IPv6 router advertisement.....	906	APN.....	723
mnc statement.....	995	mobile-pool-groups statement.....	622
mobile address pool change.....	408	mobile-pools statement.....	623
mobile address pool delete.....	410	mobile-profiles statement.....	598
mobile charging		mobility address pool delete.....	422
flags for tracing operations.....	303	mobility pool change.....	416
log filenames for tracing operations.....	303	mobility statement.....	996
tracing operations.....	302	monitoring	
mobile interface		chassis configuration.....	72
applying rewrite rules.....	319	MPCs	
mobile interface change.....	424	configuring interface MPCs.....	66
mobile interfaces		msisdn statement	
applying egress rewrite rules.....	347	service selection profiles.....	760
applying ingress rewrite rules.....	346	mtu statement	
configuring	120, 122	mobile interface.....	997
		transport profiles.....	812

- multigateway
 - P-GW configuration.....535
 - S-GW configuration.....535
- N**
- n3-requests statement
 - GTP.....948
 - GTP Prime.....813
- nbns-server statement
 - APN.....724
- network behind mobile
 - APN.....131, 133
 - P-GW.....130, 131, 133
- network element.....150
- network element group
 - configuration example.....200
 - specifying for accounting.....185
- network element groups
 - configuring.....183
 - overview.....152
- network elements
 - configuration example.....199
 - configuring.....182
 - dead server detection.....152, 181
 - load-balancing algorithm.....151
 - maximum pending requests.....152
 - overview.....151
 - server priority.....152
 - specifying for accounting.....185
 - specifying for authentication.....184
- network statement
 - mobile pools.....624
- network-behind-mobile statement.....725
- network-element statement.....600
- network-element-group statement.....600
- network-element-groups statement.....601
- network-elements statement.....602
- networks
 - 3G
 - ARP.....311
 - classifying subscriber traffic.....311
 - GBR.....311
 - MBR.....311
 - QoS parameters.....311
 - 4G
 - AMBR.....312
 - ARP.....312
 - classifying subscriber traffic.....312
 - QoS parameters.....312
- no-address-verify statement
 - APN.....725
- no-path-management statement
 - GTP Prime.....814
- no-response-cache statement.....949
- notice icons defined.....xxviii
- num-gtpu-end-markers statement.....950
- O**
- offline charging
 - configuring.....279
- offline statement
 - transport profiles.....815
 - trigger profiles.....816
- options statement
 - RADIUS.....603
- output statement
 - mobile interface.....997
- overload conditions.....457
- overview
 - interface redundancy.....76
 - physical interface types.....63
 - Routing Engine redundancy.....74
 - session DPC.....63
 - session DPC redundancy.....75
- P**
- p-cscf statement
 - APN.....726
- P-GW
 - broadband gateway.....10
 - collocated example.....525
 - collocated with S-GW.....28, 29, 525
 - function in mobile network.....40
 - functions in mobile network.....37
 - HTTP header enrichment.....134, 135
 - multigateway example.....535
 - multigateway with S-GW.....535
 - network behind mobile.....130, 131, 133
- packet data network gateway
 - functions in mobile network.....42
- packet flow
 - broadband gateway control.....6
- packet flow downlink
 - broadband gateway payload.....9
- packet flow uplink
 - broadband gateway payload.....7
- packet loss priority See PLP
- parentheses, in syntax descriptions.....xl

path management See GTP	
path-management statement	
GTP.....	951
payload flow downlink	
broadband gateway downlink.....	9
payload flow uplink	
broadband gateway uplink.....	7
PCI flags.....	314
PCRF	
mobile network.....	50
pdn-type statement	
service selection profiles.....	761
PDP contexts	
bearers.....	47
GBR.....	312
initial QoS level.....	310
MBR.....	312
upgrading based on	
ARP.....	338
highest traffic class.....	338
MBR.....	339
peer group	
configuring GTP services.....	245
peer statement	
GTP.....	952
GTP Prime.....	817
peer order	
charging gateways.....	818
service selection profiles.....	761
peer-group statement	
GTP.....	953
peer-history statement	
GTP.....	954
peer-order statement	
charging gateways.....	819
peer-routing-instance statement	
service selection profiles.....	762
pending-queue-size statement	
GTP Prime.....	820
persistent storage	
configuring.....	291
configuring the SSD.....	293, 294
disabling for charging.....	1120
ejecting the SSD.....	294
enabling for charging.....	1119
formatting SSD.....	1122
initializing the SSD.....	293
preparing SSD.....	1121, 1122
removing SSD.....	1121
tracing operations.....	292
persistent-storage-order statement.....	821
PFE charging statistics.....	453
physical interfaces	
broadband gateway.....	63
PLMN	
mobile network.....	50
PLMNs	
configuring on broadband gateway.....	11
mobile network.....	11
PLP	
mapping to QCI values.....	332
mapping to traffic classes.....	333
policer action	
configuring	
for AMBR.....	337
for GBR.....	339
for MBR.....	339
overview.....	318
policer configuration	
exceed-action.....	318
overview.....	318
violate-action.....	318
policies	
configuring on broadband gateway.....	12
pool statement	
APN.....	729
pool-name statement	
APN.....	730
dhcp.....	636
pool-prefetch-threshold statement	
mobile pools.....	625
pool-snmp-trap-threshold statement	
mobile pools.....	626
preemption	
capability.....	314
enabling.....	326
enabling.....	326
overview.....	314
PCI flags.....	314
PVI flags.....	314
vulnerability.....	314, 326
preemption statement	
GGSN or P-GW.....	884
Serving Gateway.....	885
preferred-active statement	
IPsec.....	668

prefix-v4 statement	
network behind mobile.....	727
prefix-v6 statement	
network behind mobile.....	728
primary-list statement.....	669
priority statement	
dhcp.....	637
profile statement	
service selection profiles.....	763
profile-id statement.....	822
profile-name statement	
APN.....	731
profile-selection-order statement	
APN.....	732
Serving Gateway.....	823
profiles	
configuring on broadband gateway.....	32
PVI flags.....	314

Q

QCI	
configuring.....	332
overview.....	312
QoS	
class identifiers.....	312
configuration example.....	348
configuring	
local policies.....	343
configuring on Broadband Gateway	
overview.....	323
configuring on broadband gateway.....	384
Differentiated Services model.....	310
initial level assigned to bearer.....	310
local policy	
applying at apn level.....	344
applying at system level.....	344
NQN flags and upgrade behavior.....	321
overview.....	310
traffic classes.....	311
upgrade flags and upgrade behavior.....	321
QoS and CAC	
S-GW configuration.....	385
QoS Class Identifier See QCI	
QoS classifier profiles	
configuring	
3G/4G networks.....	334
QoS local policy profiles	
APN configuration.....	119

QoS profiles	
configuring	
classifier profile.....	334
classifier profile, in 3G networks.....	333
classifier profile, in 4G networks.....	332
CoS policy profile.....	340
CoS policy profile, in 3G	
networks.....	336, 338
local policy.....	343
resource threshold profile.....	330
resource threshold profile, in 3G	
networks.....	328
resource threshold profile, in 4G	
networks.....	326
qos-class-identifier statement	
cos-cac.....	886
Quality of service See QoS	

R

RADIUS attributes.....	154
excluding or ignoring in RADIUS	
messages.....	186
supported in Access-Accept messages.....	159
supported in Access-Requests.....	155
supported in Accounting On messages.....	175
supported in Accounting Start messages.....	162
supported in Accounting Stop messages.....	171
supported in CoA messages.....	177
supported in Disconnect Request	
messages.....	176
supported in Interim-Update messages.....	166
RADIUS options.....	154
specifying in AAA profile.....	190
RADIUS servers	
assigning to network elements.....	182
configuration example.....	195
configuring.....	179
enabling dynamic requests.....	181
radius statement.....	606
range statement	
mobile pools.....	627
reachable-time statement	
IPv6 router advertisement.....	907
reconnect-time statement	
GTP Prime.....	824
redirect-peer statement	
service selection profiles.....	764
redistribute-all-traffic statement	
aggregated multiservices.....	670

redundancy	
anchor failover.....	80
broadband gateway.....	74, 75, 76
configuration example.....	82
configuring session DPC.....	76, 78
redundancy configuration example	
broadband gateway.....	82
rejecting	
maximum active bearers.....	324
rejoin-timeout statement	
aggregated multiservices.....	671
remote-delete-on-peer-fail statement	
Serving Gateway.....	998
request interface load-balancing revert (aggregated multiservices).....	1054
request interface load-balancing switchover (aggregated multiservices).....	1055
request system storage unified-edge charging media start command.....	1119
request system storage unified-edge charging media stop command.....	1120
request system storage unified-edge media eject command.....	1121
request system storage unified-edge media prepare command.....	1122
resource management	
traceoptions.....	19
resource threshold profiles	
configuring	
in 3G networks.....	328
in 3G/4G networks.....	330
in 4G networks.....	326
resource thresholds	
default settings.....	317
managing load	
bearer.....	316
CPU.....	316
memory.....	316
system.....	316
overview	316
preempting bearers.....	316
resource-management statement.....	1002
resource-threshold-profile statement	
cos-cac.....	887
local-policies.....	888
resource-triggered statement	
aggregated multiservices.....	977
response-cache-timeout statement.....	955
restart counters.....	223
restriction value	
APN configuration.....	113
restriction-value statement	
APN.....	733
retransmission-attempt statement	
dhcp.....	638
retransmission-interval statement	
dhcp.....	639
retransmission-timer statement	
IPv6 router advertisement.....	908
retry statement.....	608
revert-interval statement.....	608
rewrite rules	
default DSCP marking	
.....	346, 347
egress	
applying to mobile interfaces.....	347
configuring.....	345
overview.....	319
ingress	
applying to mobile interfaces.....	346
configuring.....	345
overview.....	319
overview.....	319
rewrite-rules statement	
class-of-service.....	889
roamer-classifier-profile statement	
local policies.....	889
roamer-cos-policy-profile statement	
local-policies.....	890
roamer-profile statement.....	734, 825
roaming users	
mobile network.....	11
route lookup	
GTP-C messages.....	225
router advertisement	
IPv6 and broadband gateway.....	92, 93
router solicitation	
IPv6 and broadband gateway.....	92, 93
router-lifetime statement	
IPv6 router advertisement.....	909
routing-instance statement	
APN.....	735
GTP.....	956
rule statement	
tag rule set.....	736

S

- S-GW
 - charging traceoptions.....284
 - collocated example.....525
 - collocated with P-GW.....28, 29, 525
 - configuring global charging profiles.....282
 - example.....385, 519
 - functions.....55
 - GTP.....249, 259, 261, 265
 - GTP traceoptions.....262
 - in mobile network.....21
 - local persistent storage traceoptions.....287
 - multigateway example.....535
 - multigateway with P-GW.....535
 - QoS and CAC.....385
 - S1 interface.....53
 - S1-U interface.....256
 - S11 interface.....252
 - S12 interface.....254
 - S4 interface.....257
 - service and tracking areas.....54
 - standalone.....519
 - traceoptions.....33
 - user packet flow.....25
- S1 interface
 - S-GW.....53
- S1-U
 - configuring.....256
- S11
 - configuring.....252
- s11 statement
 - GTP
 - Serving Gateway.....957
- S12
 - configuring.....254
- s12 statement
 - GTP.....958
- slu statement
 - GTP.....959
- S4
 - configuring.....257
- s4 statement
 - GTP.....960
- s5 interface
 - configuring GTP services
 - for GGSN/P-GW.....233
- s5 statement
 - GTP.....962
- s8 interface
 - configuring GTP services
 - for GGSN/P-GW.....235
- s8 statement
 - GTP.....964
- secondary statement
 - aggregated Packet Forwarding Engine.....672
- secret statement.....609
- selection order
 - S-GW charging configuration.....282
- selection-mode statement
 - APN.....737
- send-accounting-on statement.....609
- server statement
 - dhcp.....640
 - resource management.....1003
- servers statement.....610
- service areas
 - S-GW.....54
- service selection
 - APN configuration.....123
- service-mode statement
 - APN.....738
 - charging profiles.....826
 - gateway.....915
 - mobile pools.....628
 - Serving Gateway.....916
 - transport profiles.....828
- service-selection-profile statement
 - APN.....739
- service-selection-profiles statement.....765
- service-set statement
 - aggregated multiservices.....978
- service-set-options statement.....739
- services statement
 - dhcp.....641
- session DPC
 - anchors.....69
 - broadband gateway.....63
 - configuring.....64
 - redundancy configuration.....76
- session DPC configuration example
 - broadband gateway.....67
- session DPC redundancy configuration example
 - broadband gateway.....82
- session status.....431
- session-timeout statement
 - APN.....740

sgsn-mme-change-limit statement		
serving gateway.....	829	
sgsn-sgw-change-limit statement.....	830	
sgw statement.....	998	
shared statement		
IPsec.....	672	
show interfaces anchor-group command		
aggregated Packet Forwarding Engine.....	1056	
show interfaces load-balancing command		
aggregated multiservices.....	1059	
show services flows command		
aggregated multiservices.....	1238	
show services hcm statistics command.....	1072	
show services ipsec-vpn ipsec security-associations		
command.....	1062	
show services nat mappings app command.....	1242	
show services nat mappings eim command.....	1244	
show services nat mappings summary		
command.....	1246	
show services nat pool command		
aggregated multiservices.....	1247	
show services nat statistics command.....	1250	
show services service-sets summary		
command.....	1259	
show services sessions command		
aggregated multiservices.....	1261	
show unified edge ggsn pgw gtp statistics		
command.....	1211	
show unified edge ggsn pgw qos statistics		
command.....	1174	
show unified-edge gateways command.....	1275	
show unified-edge ggsn-pgw aaa network-element		
status command.....	1022	
show unified-edge ggsn-pgw aaa		
network-element-group status command.....	1024	
show unified-edge ggsn-pgw aaa radius statistics		
command.....	1026	
show unified-edge ggsn-pgw aaa statistics		
command.....	1035	
show unified-edge ggsn-pgw address-assignment		
group command.....	1041	
show unified-edge ggsn-pgw address-assignment		
pool command.....	1044	
show unified-edge ggsn-pgw address-assignment		
service-mode command.....	1048	
show unified-edge ggsn-pgw address-assignment		
statistics command.....	1050	
show unified-edge ggsn-pgw apn service-mode		
command.....	1079	
show unified-edge ggsn-pgw apn statistics		
command.....	1081	
show unified-edge ggsn-pgw call-rate statistics		
command.....	1277	
show unified-edge ggsn-pgw charging		
local-persistent-storage statistics		
command.....	1123	
show unified-edge ggsn-pgw charging path		
statistics command.....	1128	
show unified-edge ggsn-pgw charging path status		
command.....	1133	
show unified-edge ggsn-pgw charging service-mode		
command.....	1136	
show unified-edge ggsn-pgw charging transfer		
statistics command.....	1139	
show unified-edge ggsn-pgw charging transfer		
status command.....	1143	
show unified-edge ggsn-pgw charging		
trigger-profile command.....	1146	
show unified-edge ggsn-pgw gtp peer		
command.....	1199	
show unified-edge ggsn-pgw gtp peer statistics		
command.....	1203	
show unified-edge ggsn-pgw ip-reassembly		
statistics command.....	1186	
show unified-edge ggsn-pgw resource-manager		
clients command.....	1280	
show unified-edge ggsn-pgw service-mode		
command.....	1086	
show unified-edge ggsn-pgw statistics		
command.....	1088	
show unified-edge ggsn-pgw status		
command.....	1091	
show unified-edge ggsn-pgw status preemption-list		
command.....	1177	
show unified-edge ggsn-pgw subscribers charging		
command.....	1105	
show unified-edge ggsn-pgw subscribers		
command.....	1095	
show unified-edge ggsn-pgw system interfaces		
command.....	1066	
show unified-edge sgw call-rate statistics		
command.....	1282	
show unified-edge sgw charging path statistics		
command.....	1154	
show unified-edge sgw charging path status.....	1159	
show unified-edge sgw charging service-mode		
command.....	1162	

- show unified-edge sgw charging transfer statistics
 - command.....1164
- show unified-edge sgw charging transfer status
 - command.....1168
- show unified-edge sgw charging trigger-profile
 - command.....1170
- show unified-edge sgw gtp peer command.....1221
- show unified-edge sgw gtp peer statistics
 - command.....1225
- show unified-edge sgw gtp statistics
 - command.....1230
- show unified-edge sgw idle-mode-buffering
 - statistics command.....1286
- show unified-edge sgw ip-reassembly statistics
 - command.....1189
- show unified-edge sgw local-persistent-storage
 - statistics.....1148
- show unified-edge sgw resource-manager clients
 - command.....1290
- show unified-edge sgw service-mode
 - command.....1284
- show unified-edge sgw statistics command.....1292
- show unified-edge sgw status command.....1295
- show unified-edge sgw status preemption-list
 - command.....1180
- show unified-edge sgw subscribers charging
 - command.....1308
- show unified-edge sgw subscribers
 - command.....1300
- show unified-edge sgw system interfaces
 - command.....1068
- software-datapath statement
 - exception handling.....910
- source-interface statement.....611
 - GTP Prime.....831
 - peer.....831
- standalone
 - S-GW configuration.....519
- stop-on-access-deny statement.....611
- stop-on-failure statement.....612
- streaming traffic class
 - configuring.....334
 - description.....311
- subscriber packets
 - DSCP marking on.....346, 347
- subscriber traffic
 - policing.....318
- subscriber-awareness statement
 - service set options.....741
- support, technical See technical support
- support-16-bit-sequence statement
 - GTP.....965
- switch-back-time statement.....832
- syntax conventions.....xxxix
- system
 - managing load316
- system architecture
 - broadband gateway.....4
- system load
 - configuring.....326
 - in 3G networks.....329
 - in 3G/4G networks.....331
 - in 4G networks.....327
- system statement.....673
 - dhcp.....642
- system-load statement
 - cos-cac.....891
- T**
- t3-response statement
 - GTP.....966
 - GTP Prime.....833
- tag statement
 - HTTP header enrichment.....742
- tag-attribute statement
 - HTTP header enrichment.....743
- tag-header statement
 - HTTP header enrichment.....744
- tag-rule statement
 - HTTP header enrichment.....745
- tag-rule-set statement
 - HTTP header enrichment.....747
- tag-rule-sets statement
 - HTTP header enrichment.....748
- tag-rules statement
 - HTTP header enrichment.....746
- tag-separator statement
 - HTTP header enrichment.....748
- tariff-time-list statement.....834
- technical support
 - contacting JTAC.....xl
- TEID See tunnel endpoint identifiers
- term statement
 - service selection profiles.....766
- term-name statement
 - HTTP header enrichment.....749

then statement		overview.....	311
HTTP header enrichment.....	750	streaming.....	
service selection profiles.....	767	configuring.....	334
time-limit statement.....	835	traffic handling priority	
timeout statement.....	612	configuring.....	334
IP reassembly.....	911	traffic-class-classifier-profile statement	
trace options		cos-cac.....	892
configuring for GTP.....	247	traffic-class-cos-policy-profile statement	
trace-options-dhcp statement		cos-cac.....	893
dhcp.....	643	transport profile change.....	403, 415
traceoptions		transport profiles	
charging.....	284	configuring.....	295
datapath.....	97	transport-profile statement.....	841
exceptions.....	95	transport-profiles statement.....	843
general gateway.....	15	transport-protocol statement	
GTP.....	262	GTP Prime.....	844
local persistent storage.....	287	trigger profile change.....	405
mobile options.....	17	trigger profiles	
resource manager.....	19	configuring.....	296
S-GW.....	33	trigger statement.....	615
traceoptions statement		trigger-profile statement.....	845
Broadband Gateway.....	1004	trigger-profiles statement.....	846
charging.....	836	ttl-value statement	
local persistent storage.....	839	GTP.....	970
exception handling.....	912	Serving Gateway.....	970
GTP.....	968	tunnel endpoint identifiers.....	225
mobile options.....	1007	route lookup.....	225
resource management		tunnel management See GTP	
client.....	1009		
server.....	1012	U	
traceoptions-aaa statement.....	614	ul statement	
traceoptions-radius statement.....	613	local-policies.....	894
tracing operations		UMTS See networks	
for persistent storage.....	292	unit statement	
mobile charging.....	302	aggregated multiservices.....	674
mobile subscribers.....	302	mobile interface.....	999
tracking areas		uplink payload packet flow	
S-GW.....	54	broadband gateway.....	7
traffic classes		user types	
background		mobile network.....	11
configuring.....	334	user-name statement	
configuring.....	333	local persistent storage.....	847
GBR.....	339	user-session routing	
MBR.....	338	broadband gateway.....	107
conversational			
configuring.....	334	V	
interactive		verify-source-address statement	
configuring.....	334	APN.....	751

version statement	
GTP Prime.....	848
violate-action policer	
configuring	
for AMBR.....	337
for MBR.....	339
overview.....	318
violate-action statement	
cos-cac.....	894
visiting users	
mobile network.....	11
visitor-classifier-profile statement	
local-policies.....	895
visitor-cos-policy-profile statement	
local-policies.....	895
visitor-profile statement.....	752, 849
volume-limit statement.....	850
VRFs	
broadband gateway.....	122
VSAs	
excluding from RADIUS messages.....	186
supported.....	150

W

wait-accounting statement	
APN.....	753
configuring.....	192
warm-standby statement	
aggregated Packet Forwarding Engine.....	675
watermark-level-1 statement.....	851
watermark-level-2 statement.....	852
watermark-level-3 statement.....	853
world-readable statement	
local persistent storage.....	854

Index of Statements and Commands

A

aaa statement.....	586
APN.....	677
aaa-override statement	
APN.....	678
aaa-profile statement	
APN.....	679
aaa-radius statement.....	604
accounting statement	
unified-edge profile.....	588
accounting-port statement.....	589
accounting-secret statement.....	589
address statement.....	590
address-assignment statement	
APN.....	680
MobileNext Broadband Gateway.....	618
ageing-window statement	
mobile pools.....	619
aggregated-maximum-bit-rate statement	
cos-cac.....	855
algorithm statement.....	590
allocation and retention-priority statement	
cos-cac.....	856
allow-dynamic-requests statement.....	591
allow-network-behind-mobile statement.....	681
allow-static-ip-address statement	
APN.....	682
anchor-pfe-default-bearers-percentage statement	
Serving Gateway.....	857
anchor-pfe-guaranteed-bandwidth statement	
Serving Gateway.....	858
anchor-pfe-ipv4-nbm-prefixes statement.....	683
anchor-pfe-ipv6-nbm-prefixes statement.....	684
anchor-pfe-maximum-bearers statement	
Serving Gateway.....	859
anchor-pfes statement.....	645

anchor-service-pics statement.....	646
anchor-spics statement.....	646
anchoring-options statement.....	647
anonymous-user statement	
APN.....	685
apfe-group-set statement.....	648
apn-data-type statement	
APN.....	686
apn-name statement	
service selection profiles.....	754
apn-services statement.....	687
apn-type statement	
APN.....	690
apns statement.....	691
APN services.....	691
attributes statement.....	592
authentication statement.....	593
authentication-port statement.....	593

B

bandwidth-pool statement	
cos-cac.....	860
bearer-load statement	
cos-cac.....	861
bind-interface statement	
dhcp.....	629
block-visitors statement	
APN.....	693
broadband gateway	
interface redundancy.....	76
interfaces redundancy configuration	
example.....	82
redundancy configuration.....	74
redundancy configuration example.....	82
Routing Engine redundancy.....	74
session DPC redundancy.....	75
session DPC redundancy configuration	
example.....	82

C

call-rate-statistics statement.....	981
cdr-aggregation-limit statement.....	769
cdr-profile statement.....	770
cdr-profiles statement.....	772
cdr-release statement	
charging gateways.....	773
cds-per-file statement.....	774
charging statement.....	775
APN.....	695

charging-characteristics statement		
service selection profiles.....	755	
charging-gateways statement.....	779	
charging-profiles statement.....	780	
chassis		
redundancy configuration.....	76, 78	
class-of-service statement.....	864	
classifier-profile statement		
local-policies.....	862	
classifier-profiles statement		
cos-cac.....	863	
clear unified-edge ggsn-pgw aaa radius statistics		
command.....	1018	
clear unified-edge ggsn-pgw aaa statistics		
command.....	1019	
clear unified-edge ggsn-pgw address-assignment		
pool command.....	1020	
clear unified-edge ggsn-pgw address-assignment		
statistics command.....	1021	
clear unified-edge ggsn-pgw charging cdr		
command.....	1110	
clear unified-edge ggsn-pgw charging cdr wfa		
command.....	1111	
clear unified-edge ggsn-pgw charging		
local-persistent-storage statistics		
command.....	1112	
clear unified-edge ggsn-pgw charging path		
statistics command.....	1113	
clear unified-edge ggsn-pgw charging transfer		
statistics command.....	1114	
clear unified-edge ggsn-pgw gtp peer statistics		
command.....	1194	
clear unified-edge ggsn-pgw gtp statistics		
command.....	1196	
clear unified-edge ggsn-pgw ip-reassembly		
statistics command.....	1184	
clear unified-edge ggsn-pgw statistics		
command.....	1074	
clear unified-edge ggsn-pgw subscribers charging		
command.....	1077	
clear unified-edge ggsn-pgw subscribers		
command.....	1075	
clear unified-edge ggsn-pgw subscribers peer		
command.....	1078	
clear unified-edge sgw charging cdr		
command.....	1115	
clear unified-edge sgw charging		
local-persistent-storage statistics		
command.....	1116	
clear unified-edge sgw charging path statistics		
command.....	1117	
clear unified-edge sgw charging transfer statistics		
command.....	1118	
clear unified-edge sgw gtp peer statistics		
command.....	1197	
clear unified-edge sgw gtp statistics		
command.....	1198	
clear unified-edge sgw idle-mode-buffering		
statistics command.....	1270	
clear unified-edge sgw ip-reassembly statistics		
command.....	1185	
clear unified-edge sgw statistics command.....	1271	
clear unified-edge sgw subscribers charging		
command.....	1273	
clear unified-edge sgw subscribers		
command.....	1272	
clear unified-edge sgw subscribers peer		
command.....	1274	
client statement		
resource management.....	1000	
configuration		
broadband gateway interface PFEs.....	74	
broadband gateway services PICs.....	74	
configuration example		
redundancy.....	82	
configuring chassis		
interfaces for mobility redundancy.....	78	
session DPC redundancy.....	76	
configuring interfaces for mobility		
redundancy.....	78	
configuring redundancy		
interfaces for mobility.....	78	
session DPC.....	76	
configuring session DPC		
redundancy.....	76	
container-limit statement.....	781	
control statement		
GTP.....	917	
Gn.....	918	
Gp.....	918	
S4.....	918	
S5.....	918	
S8.....	918	
peer group.....	919	
cos-cac statement.....	865	
cos-policy-profile statement		
local-policies.....	867	

cos-policy-profiles statement		
cos-cac.....	868	
count statement		
HTTP header enrichment.....	694	
cpu statement		
cos-cac.....	869	
current-hop-limit statement		
IPv6 router advertisement.....	897	
D		
data statement		
GTP.....	920	
Gn.....	921	
Gp.....	921	
S4.....	921	
S5.....	921	
S8.....	921	
ddn-delay-sync statement.....	922	
dead-criteria-retries statement.....	594	
dead-server-retry-interval statement		
dhcp.....	630	
dead-server-successive-retry-attempt statement		
dhcp.....	631	
dedicated statement		
IPsec.....	649	
default-pool statement		
mobile pools.....	619	
default-profile statement.....	697, 782	
default-rating-group statement.....	783	
default-service-id statement.....	784	
description statement		
APN.....	698	
CDR profiles.....	785	
charging profiles.....	785	
transport profiles.....	785	
trigger profiles.....	785	
destination-address statement		
HTTP header enrichment.....	698	
destination-address-range statement		
HTTP header enrichment.....	699	
destination-ipv4-address statement		
GTP Prime.....	786	
destination-port statement		
GTP Prime.....	787	
destination-port-range statement		
HTTP header enrichment.....	699	
destination-ports statement		
HTTP header enrichment.....	700	
destination-prefix-list statement		
HTTP header enrichment.....	701	
DHCP		
configuring.....	208	
APN.....	209	
dhcp-proxy-client statement		
APN.....	702	
dhcp.....	632	
dhcp-server-selection-algorithm statement		
dhcp.....	633	
dhcpv4-profiles statement		
dhcp.....	634	
dhcpv4-proxy-client-profile statement		
APN.....	703	
dhcpv6-profiles statement		
dhcp.....	635	
dhcpv6-proxy-client-profile statement		
APN.....	704	
dial-options statement		
IPsec.....	649	
direction statement		
trigger profiles.....	788	
disable statement		
idle mode buffering.....	982	
IPv6 router advertisement.....	898	
disable-replication statement.....	789	
disk-space-policy statement.....	790	
dl-bandwidth-pool statement		
local-policies.....	870	
dns-server statement		
APN.....	705	
down-detect-time statement		
GTP Prime.....	791	
drop-member-traffic statement		
aggregated multiservices.....	650	
dscp-code-point statement		
GTP.....	923	
dscp-ipv6-rewrite-rule-name statement		
class-of-service.....	870	
dscp-ipv6-rewrite-rule-name-ingress statement		
class-of-service.....	871	
dscp-rewrite-rule-name statement		
class-of-service.....	871	
dscp-rewrite-rule-name-ingress statement		
class-of-service.....	872	
dynamic-requests-secret statement.....	594	

E

echo-interval statement	
GTP.....	924
GTP Prime.....	792
echo-n3-requests statement	
GTP.....	926
echo-t3-response statement	
GTP.....	928
egress-key statement	
aggregated multiservices.....	971
enable-reduced-partial-cdrs statement.....	793
enable-rejoin statement	
aggregated multiservices.....	651
encrypt statement	
HTTP header enrichment.....	706
error-indication-interval statement.....	898
GTP.....	930
exceed-action statement	
cos-cac.....	872
exclude statement	
RADIUS.....	595
trigger profiles.....	794
exclude-ie-options statement.....	797
exclude-pools statement	
APN.....	707
exclude-v6pools statement	
APN.....	708
expire-timer statement	
idle mode buffering.....	983
external-assigned statement	
mobile pools.....	620

F

family statement	
aggregated multiservices.....	652
mobile interface.....	983
mobile pools.....	621
file-age statement.....	801
file-creation-policy statement.....	802
file-format statement.....	803
file-name-private-extension statement.....	804
file-size statement.....	805
filter statement	
mobile interface.....	984
forwarding-class statement	
GTP.....	931
forwarding-packages statement.....	985

from statement

HTTP header enrichment.....	709
service selection profiles.....	756

G

ggsn-pgw statement.....	986
global-profile statement	
Serving Gateway.....	806
gn statement	
GTP.....	932
gp statement	
GTP.....	934
group statement	
APN.....	710
gtp statement	
GGSN.....	936
P-GW.....	936
Serving Gateway.....	941
gtpv6 statement.....	807
guaranteed-bit-rate statement	
cos-cac.....	873

H

hash-keys statement	
aggregated multiservices.....	972
hcm statement	
HTTP header enrichment.....	711
header-type statement	
GTP Prime.....	808
high statement	
cos-cac.....	874
high-availability-options statement	
aggregated multiservices.....	653
history statement	
call-rate statistics.....	986
home-plmn statement.....	987
home-profile statement.....	712, 809

I

idle-mode-buffering statement.....	988
idle-timeout statement	
APN.....	713
idle-timeout-direction statement	
APN.....	714
ignore statement.....	597
imei statement	
service selection profiles.....	757

imsi statement		
network behind mobile.....	715	
service selection profiles.....	758	
indirect-tunnel statement.....	945	
inet-pool statement		
APN.....	716	
inet-precedence-rewrite-rule-name statement		
class-of-service.....	874	
inet-precedence-rewrite-rule-name-ingress statement		
class-of-service.....	875	
inet6-pool statement		
APN.....	717	
ingress-key statement		
aggregated multiservices.....	974	
ingress-rewrite-rules statement		
class of service.....	875	
input statement		
mobile interface.....	988	
inter-mobile-traffic statement		
APN.....	718	
interface redundancy configuration example		
broadband gateway.....	82	
interface statement.....	989	
anchor Packet Forwarding Engine.....	654	
GTP.....	946	
services PIC.....	656	
session PIC.....	657	
interface-service statement		
aggregated multiservices.....	975	
interfaces for mobility		
redundancy configuration.....	78	
interfaces statement		
aggregated multiservices.....	658	
aggregated Packet Forwarding Engine.....	660	
class-of-service.....	876	
mobile interface.....	990	
interval statement		
call-rate statistics.....	991	
ip-reassembly statement.....	899	
ip-reassembly-profile statement.....	900	
ipsec-interface-id statement		
IPsec.....	661	
ipv6-router-advertisement statement.....	901	
L		
lease-time statement		
dhcp.....	636	
load-balancing-options statement		
aggregated multiservices.....	662, 976	
IPsec.....	663	
local statement		
APN.....	719	
local-persistent-storage-options statement.....	810	
local-policies.....	877	
local-policy-profile statement		
APN.....	720	
Broadband Gateway.....	878, 992	
local-storage statement.....	811	
logical-system statement		
APN.....	721	
low statement		
cos-cac.....	879	
M		
many-to-one statement		
aggregated multiservices.....	664	
max-reassembly-pending-packets statement		
IP reassembly.....	902	
maximum-advertisement-interval statement		
IPv6 router advertisement.....	903	
maximum-bearers statement		
APN.....	722	
Broadband Gateway.....	880, 993	
service selection profiles.....	759	
maximum-bit-rate statement		
cos-cac.....	881	
maximum-initial-advertisement-interval statement		
IPv6 router advertisement.....	904	
maximum-initial-advertisements statement		
IPv6 router advertisement.....	905	
maximum-pending-reqs-limit statement.....	597	
mcc statement.....	994	
member-failure-options statement		
aggregated multiservices.....	665	
member-interface statement		
aggregated multiservices.....	667	
memory statement		
cos-cac.....	882	
mif statement		
class of service.....	883	
minimum-advertisement-interval statement		
IPv6 router advertisement.....	906	
mnc statement.....	995	
mobile options statement.....	1001	
mobile-interface statement		
APN.....	723	

mobile-pool-groups statement.....	622
mobile-pools statement.....	623
mobile-profiles statement.....	598
mobility statement.....	996
msisdn statement	
service selection profiles.....	760
mtu statement	
mobile interface.....	997
transport profiles.....	812

N

n3-requests statement	
GTP.....	948
GTP Prime.....	813
nbns-server statement	
APN.....	724
network statement	
mobile pools.....	624
network-behind-mobile statement.....	725
network-element statement.....	600
network-element-group statement.....	600
network-element-groups statement.....	601
network-elements statement.....	602
no-address-verify statement	
APN.....	725
no-path-management statement	
GTP Prime.....	814
no-response-cache statement.....	949
num-gtpu-end-markers statement.....	950

O

offline statement	
transport profiles.....	815
trigger profiles.....	816
options statement	
RADIUS.....	603
output statement	
mobile interface.....	997
overview	
interface redundancy.....	76
Routing Engine redundancy.....	74
session DPC redundancy.....	75

P

p-cscf statement	
APN.....	726
path-management statement	
GTP.....	951

pdn-type statement	
service selection profiles.....	761
peer statement	
GTP.....	952
GTP Prime.....	817
peer order	
charging gateways.....	818
service selection profiles.....	761
peer-group statement	
GTP.....	953
peer-history statement	
GTP.....	954
peer-order statement	
charging gateways.....	819
peer-routing-instance statement	
service selection profiles.....	762
pending-queue-size statement	
GTP Prime.....	820
persistent-storage-order statement.....	821
pool statement	
APN.....	729
pool-name statement	
APN.....	730
dhcp.....	636
pool-prefetch-threshold statement	
mobile pools.....	625
pool-snmp-trap-threshold statement	
mobile pools.....	626
preemption statement	
GGSN or P-GW.....	884
Serving Gateway.....	885
preferred-active statement	
IPsec.....	668
prefix-v4 statement	
network behind mobile.....	727
prefix-v6 statement	
network behind mobile.....	728
primary-list statement.....	669
priority statement	
dhcp.....	637
profile statement	
service selection profiles.....	763
profile-id statement.....	822
profile-name statement	
APN.....	731
profile-selection-order statement	
APN.....	732
Serving Gateway.....	823

Q

qos-class-identifier statement	
cos-cac.....	886

R

radius statement.....	606
range statement	
mobile pools.....	627
reachable-time statement	
IPv6 router advertisement.....	907
reconnect-time statement	
GTP Prime.....	824
redirect-peer statement	
service selection profiles.....	764
redistribute-all-traffic statement	
aggregated multiservices.....	670
redundancy	
broadband gateway.....	74, 75, 76
configuration example.....	82
configuring session DPC.....	76, 78
redundancy configuration example	
broadband gateway.....	82
rejoin-timeout statement	
aggregated multiservices.....	671
remote-delete-on-peer-fail statement	
Serving Gateway.....	998
request interface load-balancing revert (aggregated multiservices).....	1054
request interface load-balancing switchover (aggregated multiservices).....	1055
request system storage unified-edge charging media start command.....	1119
request system storage unified-edge charging media stop command.....	1120
request system storage unified-edge media eject command.....	1121
request system storage unified-edge media prepare command.....	1122
resource-management statement.....	1002
resource-threshold-profile statement	
cos-cac.....	887
local-policies.....	888
resource-triggered statement	
aggregated multiservices.....	977
response-cache-timeout statement.....	955
restriction-value statement	
APN.....	733
retransmission-attempt statement	
dhcp.....	638

retransmission-interval statement	
dhcp.....	639
retransmission-timer statement	
IPv6 router advertisement.....	908
retry statement.....	608
revert-interval statement.....	608
rewrite-rules statement	
class-of-service.....	889
roamer-classifier-profile statement	
local policies.....	889
roamer-cos-policy-profile statement	
local-policies.....	890
roamer-profile statement.....	734, 825
router-lifetime statement	
IPv6 router advertisement.....	909
routing-instance statement	
APN.....	735
GTP.....	956
rule statement	
tag rule set.....	736

S

s11 statement	
GTP	
Serving Gateway.....	957
s12 statement	
GTP.....	958
s1u statement	
GTP.....	959
s4 statement	
GTP.....	960
s5 statement	
GTP.....	962
s8 statement	
GTP.....	964
secondary statement	
aggregated Packet Forwarding Engine.....	672
secret statement.....	609
selection-mode statement	
APN.....	737
send-accounting-on statement.....	609
server statement	
dhcp.....	640
resource management.....	1003
servers statement.....	610
service-mode statement	
APN.....	738
charging profiles.....	826
gateway.....	915

mobile pools.....	628	show unified-edge ggsn-pgw aaa network-element status command.....	1022
Serving Gateway.....	916	show unified-edge ggsn-pgw aaa network-element-group status command.....	1024
transport profiles.....	828	show unified-edge ggsn-pgw aaa radius statistics command.....	1026
service-selection-profile statement		show unified-edge ggsn-pgw aaa statistics command.....	1035
APN.....	739	show unified-edge ggsn-pgw address-assignment group command.....	1041
service-selection-profiles statement.....	765	show unified-edge ggsn-pgw address-assignment pool command.....	1044
service-set statement		show unified-edge ggsn-pgw address-assignment service-mode command.....	1048
aggregated multiservices.....	978	show unified-edge ggsn-pgw address-assignment statistics command.....	1050
service-set-options statement.....	739	show unified-edge ggsn-pgw apn service-mode command.....	1079
services statement		show unified-edge ggsn-pgw apn statistics command.....	1081
dhcp.....	641	show unified-edge ggsn-pgw call-rate statistics command.....	1277
session DPC		show unified-edge ggsn-pgw charging local-persistent-storage statistics command.....	1123
redundancy configuration.....	76	show unified-edge ggsn-pgw charging path statistics command.....	1128
session DPC redundancy configuration example		show unified-edge ggsn-pgw charging path status command.....	1133
broadband gateway.....	82	show unified-edge ggsn-pgw charging service-mode command.....	1136
session-timeout statement		show unified-edge ggsn-pgw charging transfer statistics command.....	1139
APN.....	740	show unified-edge ggsn-pgw charging transfer status command.....	1143
sgsn-mme-change-limit statement		show unified-edge ggsn-pgw charging trigger-profile command.....	1146
serving gateway.....	829	show unified-edge ggsn-pgw gtp peer command.....	1199
sgsn-sgw-change-limit statement.....	830	show unified-edge ggsn-pgw gtp peer statistics command.....	1203
sgw statement.....	998	show unified-edge ggsn-pgw ip-reassembly statistics command.....	1186
shared statement		show unified-edge ggsn-pgw resource-manager clients command.....	1280
IPsec.....	672	show unified-edge ggsn-pgw service-mode command.....	1086
show interfaces anchor-group command		show unified-edge ggsn-pgw statistics command.....	1088
aggregated Packet Forwarding Engine.....	1056		
show interfaces load-balancing command			
aggregated multiservices.....	1059		
show services flows command			
aggregated multiservices.....	1238		
show services hcm statistics command.....	1072		
show services ipsec-vpn ipsec security-associations command.....	1062		
show services nat mappings app command.....	1242		
show services nat mappings eim command.....	1244		
show services nat mappings summary command.....	1246		
show services nat pool command			
aggregated multiservices.....	1247		
show services nat statistics command.....	1250		
show services service-sets summary command.....	1259		
show services sessions command			
aggregated multiservices.....	1261		
show unified edge ggsn pgw gtp statistics command.....	1211		
show unified edge ggsn pgw qos statistics command.....	1174		
show unified-edge gateways command.....	1275		

show unified-edge ggsn-pgw status command.....	1091
show unified-edge ggsn-pgw status preemption-list command.....	1177
show unified-edge ggsn-pgw subscribers charging command.....	1105
show unified-edge ggsn-pgw subscribers command.....	1095
show unified-edge ggsn-pgw system interfaces command.....	1066
show unified-edge sgw call-rate statistics command.....	1282
show unified-edge sgw charging path statistics command.....	1154
show unified-edge sgw charging path status.....	1159
show unified-edge sgw charging service-mode command.....	1162
show unified-edge sgw charging transfer statistics command.....	1164
show unified-edge sgw charging transfer status command.....	1168
show unified-edge sgw charging trigger-profile command.....	1170
show unified-edge sgw gtp peer command.....	1221
show unified-edge sgw gtp peer statistics command.....	1225
show unified-edge sgw gtp statistics command.....	1230
show unified-edge sgw idle-mode-buffering statistics command.....	1286
show unified-edge sgw ip-reassembly statistics command.....	1189
show unified-edge sgw local-persistent-storage statistics.....	1148
show unified-edge sgw resource-manager clients command.....	1290
show unified-edge sgw service-mode command.....	1284
show unified-edge sgw statistics command.....	1292
show unified-edge sgw status command.....	1295
show unified-edge sgw status preemption-list command.....	1180
show unified-edge sgw subscribers charging command.....	1308
show unified-edge sgw subscribers command.....	1300
show unified-edge sgw system interfaces command.....	1068
software-datapath statement exception handling.....	910
source-interface statement.....	611
GTP Prime.....	831
peer.....	831
stop-on-access-deny statement.....	611
stop-on-failure statement.....	612
subscriber-awareness statement service set options.....	741
support-16-bit-sequence statement GTP.....	965
switch-back-time statement.....	832
system statement.....	673
dhcp.....	642
system-load statement cos-cac.....	891
T	
t3-response statement GTP.....	966
GTP Prime.....	833
tag statement HTTP header enrichment.....	742
tag-attribute statement HTTP header enrichment.....	743
tag-header statement HTTP header enrichment.....	744
tag-rule statement HTTP header enrichment.....	745
tag-rule-set statement HTTP header enrichment.....	747
tag-rule-sets statement HTTP header enrichment.....	748
tag-rules statement HTTP header enrichment.....	746
tag-separator statement HTTP header enrichment.....	748
tariff-time-list statement.....	834
term statement service selection profiles.....	766
term-name statement HTTP header enrichment.....	749
then statement HTTP header enrichment.....	750
service selection profiles.....	767
time-limit statement.....	835
timeout statement.....	612
IP reassembly.....	911

trace-options-dhcp statement		visitor-profile statement.....752, 849
dhcp.....	643	volume-limit statement.....850
traceoptions statement		
Broadband Gateway.....	1004	
charging.....	836	
local persistent storage.....	839	
exception handling.....	912	
GTP.....	968	
mobile options.....	1007	
resource management		
client.....	1009	
server.....	1012	
traceoptions-aaa statement.....	614	
traceoptions-radius statement.....	613	
traffic-class-classifier-profile statement		
cos-cac.....	892	
traffic-class-cos-policy-profile statement		
cos-cac.....	893	
transport-profile statement.....	841	
transport-profiles statement.....	843	
transport-protocol statement		
GTP Prime.....	844	
trigger statement.....	615	
trigger-profile statement.....	845	
trigger-profiles statement.....	846	
ttl-value statement		
GTP.....	970	
Serving Gateway.....	970	
U		
ul statement		
local-policies.....	894	
unit statement		
aggregated multiservices.....	674	
mobile interface.....	999	
user-name statement		
local persistent storage.....	847	
V		
verify-source-address statement		
APN.....	751	
version statement		
GTP Prime.....	848	
violate-action statement		
cos-cac.....	894	
visitor-classifier-profile statement		
local-policies.....	895	
visitor-cos-policy-profile statement		
local-policies.....	895	