

MobileNext Broadband Gateway Configuration Guide

Release

11.2



Published: 2011-12-06

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 | xxix |
| Part 1 | Overview | |
| Chapter 1 | System Architecture | 3 |
| Chapter 2 | Network Architecture | 21 |
| Part 2 | System Configuration | |
| Chapter 3 | Configuring Mobility on MX 3D Devices | 37 |
| Chapter 4 | Configuring Redundancy on MX 3D Devices | 49 |
| Chapter 5 | Configuring Mobile Edge Exception Handling | 63 |
| Part 3 | APN Configuration | |
| Chapter 6 | Configuring APNs | 79 |
| Part 4 | Authorization and Addressing Configuration | |
| Chapter 7 | Configuring AAA | 107 |
| Chapter 8 | Configuring DHCP | 167 |
| Part 5 | GPRS Tunneling Protocol (GTP) Configuration | |
| Chapter 9 | Configuring GTP | 173 |
| Part 6 | Charging Configuration | |
| Chapter 10 | Charging Overview | 211 |
| Chapter 11 | Configuring Charging | 219 |
| Part 7 | Quality of Service Configuration | |
| Chapter 12 | Configuring Quality of Service | 239 |
| Part 8 | Maintenance | |
| Chapter 13 | Maintenance Mode | 317 |
| Part 9 | Monitoring and Troubleshooting | |
| Chapter 14 | Monitoring | 353 |
| Chapter 15 | Troubleshooting | 381 |

| | | |
|------------|--|------|
| Part 10 | Examples | |
| Chapter 16 | Example Configurations | 395 |
| Part 11 | Complete Configuration Statement Hierarchy and Summary of Statements | |
| Chapter 17 | Configuration Statement Hierarchy | 447 |
| Chapter 18 | AAA on the Broadband Gateway | 469 |
| Chapter 19 | Address Assignment and DHCP Configuration Statements | 501 |
| Chapter 20 | Anchor Packet Forwarding Engine Redundancy and Aggregated Multiservices High Availability Configuration Statements | 529 |
| Chapter 21 | APN Configuration Statements | 553 |
| Chapter 22 | Charging Configuration Statements | 619 |
| Chapter 23 | Class of Service (CoS) Configuration Statements | 693 |
| Chapter 24 | Exception Handling Configuration Statements | 731 |
| Chapter 25 | Gateway Maintenance Mode Configuration Statement | 749 |
| Chapter 26 | GTP Configuration Statements | 751 |
| Chapter 27 | Service Applications Configuration Statements | 771 |
| Chapter 28 | System Architecture and Gateway Traceoptions Configuration Statements | 779 |
| Part 12 | Command Reference | |
| Chapter 29 | AAA Operational Commands | 809 |
| Chapter 30 | Anchor Packet Forwarding Engine Redundancy and Aggregated Multiservices High Availability Operational Commands | 833 |
| Chapter 31 | APN and Related Operational Commands | 845 |
| Chapter 32 | Charging Operational Commands | 875 |
| Chapter 33 | Class of Service (CoS) Operational Commands | 957 |
| Chapter 34 | Exception Handling Operational Commands | 963 |
| Chapter 35 | GPRS Tunneling Protocol (GTP) Operational Commands | 973 |
| Chapter 36 | Service Applications Operational Commands | 981 |
| Chapter 37 | System Architecture Operational Commands | 1013 |
| Part 13 | Index | |
| | Index | 1021 |
| | Index of Statements and Commands | 1039 |

Table of Contents

| | | |
|------------------|---|-------------|
| | About This Guide | xxix |
| | Junos Documentation and Release Notes | xxix |
| | Objectives | xxx |
| | Audience | xxx |
| | Supported Platforms | xxx |
| | Using the Indexes | xxxi |
| | Using the Examples in This Manual | xxxi |
| | Merging a Full Example | xxxi |
| | Merging a Snippet | xxxii |
| | Documentation Conventions | xxxii |
| | Documentation Feedback | xxxiv |
| | Requesting Technical Support | xxxiv |
| | Self-Help Online Tools and Resources | xxxv |
| | Opening a Case with JTAC | xxxv |
| Part 1 | Overview | |
| Chapter 1 | System Architecture | 3 |
| | Overview of Broadband Gateway System Architecture | 3 |
| | Overview of Broadband Gateway System Control Packet Flow | 5 |
| | Overview of Broadband Gateway Uplink Payload Packet Flow | 7 |
| | Overview of Broadband Gateway Downlink Payload Packet Flow | 8 |
| | Overview of Broadband Gateway as GGSN or P-GW | 9 |
| | Understanding Mobile User Types | 10 |
| | Configuring Broadband Gateway Home PLMNs and Gateways | 10 |
| | Configuring Broadband Gateway Local Policies Application | 11 |
| | Configuring Broadband Gateway Call Rate Statistics | 13 |
| | Verifying the Gateway Configuration | 13 |
| | Configuring General Gateway Trace Options | 14 |
| | Configuring Mobile Options Trace Options | 16 |
| | Configuring Resource Manager Trace Options | 18 |
| Chapter 2 | Network Architecture | 21 |
| | Overview of Mobile Networks | 21 |
| | Overview of 3G Mobile Networks and the MobileNext Broadband Gateway | 22 |
| | Overview of GGSN and P-GW | 24 |
| | Overview of Packet Data Network Gateway Functions | 25 |
| | Overview of the Evolved Packet Core | 26 |
| | Overview of APNs | 28 |
| | Overview of PDP Contexts and Bearers | 30 |
| | Overview of GGSN and Broadband Gateway Deployment | 31 |

| | | |
|------------------|--|-----------|
| | Overview of 4G/LTE and Broadband Gateway Deployment | 32 |
| | Overview of IPv6 and the Broadband Gateway | 34 |
| Part 2 | System Configuration | |
| Chapter 3 | Configuring Mobility on MX 3D Devices | 37 |
| | MobileNext Broadband Gateway Chassis Overview | 38 |
| | Session DPCs for Mobility | 39 |
| | Overview of Mobility Interface Types | 39 |
| | Configuring Session DPCs for Mobility | 40 |
| | Configuring Interface DPCs or MPCs for User Mobility Traffic | 42 |
| | Example: Configuring the MobileNext Broadband Gateway Chassis | 43 |
| | Understanding the MobileNext Broadband Gateway Anchors | 45 |
| | Configuring Anchor Session DPCs and PFEs | 47 |
| | Verifying the MobileNext Broadband Gateway Chassis Configuration | 48 |
| Chapter 4 | Configuring Redundancy on MX 3D Devices | 49 |
| | Broadband Gateway Redundancy Overview | 50 |
| | Routing Engine Redundancy | 50 |
| | Session DPC Redundancy | 51 |
| | Interface Redundancy | 52 |
| | Configuring Session DPC Redundancy | 52 |
| | Configuring Interface Redundancy | 54 |
| | Understanding the Broadband Gateway Anchor Failover Behavior | 56 |
| | Example: Configuring Broadband Gateway Redundancy | 58 |
| Chapter 5 | Configuring Mobile Edge Exception Handling | 63 |
| | Understanding the Broadband Gateway Exception Handling | 64 |
| | Understanding GTP-U Error Exception Handling | 65 |
| | Understanding Broadband Gateway IP Fragment Handling | 66 |
| | Configuring Fragment Reassembly Parameters | 66 |
| | Understanding IPv6 Protocol Parameters | 67 |
| | Configuring IPv6 Protocol Parameters | 68 |
| | Configuring Exception Handling Traceoptions | 70 |
| | Example: Configuring Broadband Gateway Exception Handling Parameters | 72 |
| Part 3 | APN Configuration | |
| Chapter 6 | Configuring APNs | 79 |
| | Configuring APNs on the MobileNext Broadband Gateway Overview | 79 |
| | General APN Parameters | 80 |
| | Restriction Value | 80 |
| | Anonymous Users | 81 |
| | Address Assignment | 81 |
| | Anchor DPC or MPC Failure Behavior | 81 |
| | Charging Profiles | 81 |
| | User-Session Routing Overview | 81 |
| | Configuring General APN Parameters on the Broadband Gateway | 83 |
| | Configuring the APN Name, Interface, and Type | 83 |
| | Configuring Servers for an APN | 84 |

| | | |
|------------------|--|------------|
| | Configuring APN Timers | 85 |
| | Configuring Miscellaneous APN Parameters | 85 |
| | Configuring the Restriction Value on a Broadband Gateway APN | 87 |
| | Configuring Anonymous Users on a Broadband Gateway APN | 88 |
| | Configuring Address Assignment on a Broadband Gateway APN | 89 |
| | Configuring Charging and Local Policy Profiles on a Broadband Gateway APN | 93 |
| | Configuring Mobile Interfaces for APNs | 94 |
| | Configuring Mobile Interface to APN Associations in VRFs | 96 |
| | Configuring APN Service Selection on a Broadband Gateway | 97 |
| | Example: Configuring Broadband Gateway APNs | 100 |
| Part 4 | Authorization and Addressing Configuration | |
| Chapter 7 | Configuring AAA | 107 |
| | Overview of AAA on the Broadband Gateway | 108 |
| | Authentication | 108 |
| | Accounting | 109 |
| | APN-Specific AAA Settings | 109 |
| | RADIUS-Initiated Dynamic Requests | 110 |
| | Support for RADIUS Attributes, Juniper Networks VSAs, and 3GPP VSAs | 110 |
| | Scalability and Redundancy | 110 |
| | Scalability | 110 |
| | Redundancy | 111 |
| | Network Elements | 111 |
| | Load Balancing Within Network Elements | 111 |
| | Server Priority | 112 |
| | Dead Server Detection | 112 |
| | Maximum Pending Requests for a Network Element | 112 |
| | Network Element Groups | 112 |
| | AAA Profiles | 113 |
| | Authentication Options | 113 |
| | Accounting Options | 113 |
| | RADIUS Attributes to Ignore or Exclude | 114 |
| | RADIUS Options | 114 |
| | Supported Attributes in Access-Request Messages | 115 |
| | RADIUS IETF Attributes Supported in Access-Request Messages | 115 |
| | 3GPP VSAs Supported in Access-Request Messages | 117 |
| | Supported Attributes in Access-Accept Messages | 119 |
| | RADIUS IETF Attributes Supported in Access-Accept Messages | 120 |
| | 3GPP VSAs Supported in Access-Accept Messages | 121 |
| | Juniper Networks VSAs Supported in Access-Accept Messages | 122 |
| | Supported Attributes in Accounting Start Messages | 122 |
| | RADIUS IETF Attributes Supported in Accounting Start Messages | 122 |
| | 3GPP VSAs Supported in Accounting Start Messages | 124 |
| | Supported Attributes in Accounting Interim Update Messages | 126 |
| | RADIUS IETF Attributes Supported in Interim-Update Messages | 126 |
| | 3GPP VSAs Supported in Interim-Update Messages | 128 |

| | | |
|------------------|--|------------|
| | Supported Attributes in Accounting Stop Messages | 131 |
| | RADIUS IETF Attributes Supported in Accounting Stop Messages | 131 |
| | 3GPP VSAs Supported in Accounting Stop Messages | 133 |
| | Supported Attributes in Accounting On Messages | 135 |
| | RADIUS IETF Attributes Supported in Accounting On Messages | 135 |
| | Supported Attributes in Disconnect Request Messages | 136 |
| | RADIUS IETF Attributes Supported in Disconnect Request Messages | 136 |
| | 3GPP VSAs Supported in Disconnect Request Messages | 137 |
| | Supported Attributes in Change of Authorization (CoA) Messages | 137 |
| | RADIUS IETF Attributes Supported in CoA Messages | 137 |
| | 3GPP VSAs Supported in CoA Messages | 138 |
| | Configuring AAA on the Broadband Gateway | 139 |
| | Configuring Interaction Between the Broadband Gateway and RADIUS Servers | 139 |
| | Configuring RADIUS-Initiated Dynamic Request Support | 141 |
| | Configuring Dead Server Detection | 141 |
| | Configuring Network Elements | 142 |
| | Configuring Network Element Groups | 143 |
| | Configuring an AAA Profile | 144 |
| | Configuring Authentication Settings in an AAA Profile | 144 |
| | Configuring Accounting Settings in an AAA Profile | 145 |
| | Configuring RADIUS Attribute Usage for an AAA Profile | 146 |
| | Specifying RADIUS Options in an AAA Profile | 150 |
| | Applying an AAA Profile to an APN | 150 |
| | Enabling Address Assignment by the RADIUS Server | 151 |
| | Configuring AAA-Assigned Addresses to Override Locally or DHCP-Assigned Addresses | 151 |
| | Configuring the Broadband Gateway to Wait for an Accounting Response | 152 |
| | Example: Configuring AAA on the Broadband Gateway | 152 |
| Chapter 8 | Configuring DHCP | 167 |
| | DHCP Overview | 167 |
| | DHCP Protocol | 167 |
| | DHCP Proxy Client | 168 |
| | Configuring DHCP Proxy Client | 168 |
| | Configuring DHCP Under APN | 169 |
| Part 5 | GPRS Tunneling Protocol (GTP) Configuration | |
| Chapter 9 | Configuring GTP | 173 |
| | GTP Versions and GPRS Interfaces Overview | 174 |
| | GPRS Tunneling Protocol (GTP) Overview | 175 |
| | GTP Path Management Overview | 176 |
| | Default Path Management Configuration | 176 |
| | GTP Version Support for Echo Requests and Echo Responses | 177 |
| | Understanding Path Management | 177 |
| | Successful Echo-Request Sequence for Path Management | 177 |
| | Failed Echo Request Sequence for Path Management | 178 |

| | |
|---|-----|
| GTP Tunnel Management Overview | 180 |
| GTP Tunnel Management Functions | 180 |
| Default Tunnel Management Configuration | 180 |
| GTP Version Support for Tunnel Management Requests and Responses .. | 180 |
| Understanding Tunnel Management | 181 |
| Successful Create Request Sequence for Tunnel Management | 181 |
| Successful Update/Delete Request Sequence for Tunnel Management ... | 181 |
| Failed Update/Delete Request Sequence for Tunnel Management | 182 |
| Restart Counters Overview | 183 |
| Understanding CSID Signaling | 184 |
| Understanding Tunnel Endpoint Identifiers | 185 |
| Configuring GTP Services Overview | 186 |
| GTP-C and GTP-U Path Management | 186 |
| Configuring GTP Services at Different Levels on a Broadband Gateway ... | 186 |
| GTP Services Default Settings | 187 |
| GTP Version Support | 188 |
| Configuring a Loopback Interface for Transport of GTP Packets | 188 |
| Configuring GTP Services on a Broadband Gateway | 189 |
| Configuring GTP Services on the Control Plane | 190 |
| Configuring GTP Services on the Data Plane | 192 |
| Configuring GTP Services on the S5 Interface | 193 |
| Configuring GTP Services on the S8 Interface | 195 |
| Configuring GTP Services on the Gn Interface | 196 |
| Configuring GTP Services on the Gp Interface | 198 |
| Configuring GTP Services When the S5 and S8 Interfaces Are in Different VRFs | 199 |
| Configuring GTP Services When the S5 and S8 Interfaces Are in the Same VRF | 201 |
| Configuring GTP Services When 3GPP Interfaces Are in Different VRFs | 202 |
| Configuring GTP Services on a GGSN Broadband Gateway | 204 |
| Configuring GTP Services on a Peer Group | 205 |
| Disabling Path Management on a Broadband Gateway or Peer Group | 206 |
| Configuring GTP Trace Options | 207 |

Part 6

Chapter 10

Charging Configuration

| | |
|---|------------|
| Charging Overview | 211 |
| Charging | 211 |
| Charging Services Overview | 211 |
| Charging Data Records | 213 |
| Information Collection and CDR Generation | 215 |
| CDR Delivery | 216 |
| Charging Profiles | 217 |
| Charging Profile Selection Process | 217 |

| | | |
|-------------------|---|------------|
| Chapter 11 | Configuring Charging | 219 |
| | Configuring Charging | 219 |
| | Configuring GTP Prime for Charging | 220 |
| | Configuring GTP Prime for Transferring CDRs | 220 |
| | Configuring GTP Prime Peers | 221 |
| | Configuring Persistent Storage | 222 |
| | Configuring Local Persistent Storage | 222 |
| | Tracing Persistent Storage Operations | 223 |
| | Configuring the Solid State Disk for Persistent Storage | 224 |
| | Initializing the Solid State Disk for Persistent Storage | 225 |
| | Ejecting the Solid State Disk | 225 |
| | Installing the Solid State Disk | 225 |
| | Configuring Transport Profiles | 226 |
| | Configuring Charging Trigger Events | 227 |
| | Configuring CDR Attributes | 229 |
| | Configuring Charging Profiles | 231 |
| | Configuring Charging Profiles for APNs | 232 |
| | Tracing Charging Operations | 233 |
| | Configuring the Trace Log Filename | 233 |
| | Configuring the Tracing Flags | 234 |
| | Verifying and Managing the Charging Configuration | 235 |
| | | |
| Part 7 | Quality of Service Configuration | |
| Chapter 12 | Configuring Quality of Service | 239 |
| | Quality of Service Overview | 240 |
| | Initial QoS | 240 |
| | Differentiated Services | 240 |
| | QoS Parameters in 3G Networks | 241 |
| | QoS Parameters in 4G Networks | 242 |
| | Aggregate Maximum Bit Rate | 244 |
| | Allocation and Retention Priority | 244 |
| | Preemption | 244 |
| | Call Admission Control Overview | 245 |
| | Enforcing Call Admission Control | 245 |
| | Managing Bandwidth | 245 |
| | Managing the Number of Bearers | 246 |
| | Managing Resource Thresholds | 246 |
| | Default Resource Threshold Settings | 247 |
| | Class of Service (CoS) Policy Profile Overview | 247 |
| | Policing Subscriber Traffic on the Broadband Gateway Overview | 248 |
| | Applying Rewrite Rules on Mobile Interfaces Overview | 249 |
| | Understanding Upstream and Downstream Processing of ToS Values in GTP-U | |
| | Packets | 250 |
| | Processing of ToS Values for Upstream Subscriber Packets | 250 |
| | Processing of ToS Values for Downstream Subscriber Packets | 251 |
| | Understanding How NQN and Upgrade Flags in PDP Contexts Affect QoS | |
| | Upgrade Behavior | 251 |

| | |
|--|-----|
| Configuring QoS on the Broadband Gateway Overview | 253 |
| Configuring the Maximum Number of Bearers | 254 |
| Configuring Bandwidth Pools | 255 |
| Configuring Preemption for Call Admission Control | 256 |
| Configuring Resource Thresholds on a 4G Network | 256 |
| Configuring Resource Thresholds on a 3G Network | 258 |
| Configuring Resource Thresholds for 3G and 4G Networks | 260 |
| Configuring a Classifier Profile for a 4G Network | 262 |
| Configuring a Classifier Profile for a 3G Network | 263 |
| Configuring a Classifier Profile for 3G and 4G Networks | 264 |
| Configuring a CoS Policy Profile for a 4G Network | 266 |
| Configuring a CoS Policy Profile for a 3G Network | 268 |
| Configuring a CoS Policy Profile for 3G and 4G Networks | 270 |
| Configuring a Local Policy | 273 |
| Applying a Local Policy | 274 |
| Configuring Ingress Rewrite Rules for a Mobile Interface | 274 |
| Configuring Egress Rewrite Rules for a Mobile Interface | 275 |
| Applying Ingress Rewrite Rules to a Mobile Interface | 276 |
| Applying Egress Rewrite Rules to Mobile Interfaces | 276 |
| Example: Configuring Quality of Service | 277 |

Part 8

Chapter 13

Maintenance

| | |
|---|------------|
| Maintenance Mode | 317 |
| Mobility Maintenance Mode Overview | 318 |
| Changing a GTP Interface Address | 319 |
| Deleting a GTP Interface | 320 |
| Modifying an Access Point Name | 322 |
| Configuring the Mobile Interface of an Access Point Name | 323 |
| Deleting an Access Point Name | 325 |
| Changing a Charging Profile | 326 |
| Changing a Transport Profile | 327 |
| Changing a Trigger Profile | 329 |
| Deleting a Charging Profile | 330 |
| Changing a Call Detail Record Profile in a Charging Profile | 331 |
| Changing Address Attributes in the Mobile Address Pool | 332 |
| Deleting a Mobile Address Pool | 334 |
| Example: Changing Access Point Name Values | 335 |
| Example: Deleting an APN | 336 |
| Example: Changing a Charging Profile | 337 |
| Example: Changing a Transport Profile | 339 |
| Example: Changing Mobility Pool Attributes | 340 |
| Example: Deleting a Mobility Address Pool | 346 |
| Example: Modifying Mobile Interface Parameters | 347 |

| | | |
|-------------------|---|------------|
| Part 9 | Monitoring and Troubleshooting | |
| Chapter 14 | Monitoring | 353 |
| | Monitoring the Mobile Environment – Key Performance Indicators | 353 |
| | Monitoring Resources | 354 |
| | Monitoring GTP Signaling | 354 |
| | Monitoring Session Status | 355 |
| | Monitoring CPU Indicators | 356 |
| | Monitoring Memory Indicators | 357 |
| | Monitoring Charging Gateways | 357 |
| | Monitoring Data Path Measurements | 359 |
| | Monitoring Call Rate Statistics | 359 |
| | Monitoring Data Rate Statistics | 359 |
| | Tracing Control Packets | 362 |
| | How to Trace Data Packets from Gn to Gi Interfaces | 366 |
| | Trace Data Packets from Gi to Gn Interfaces | 370 |
| | How to Verify Charging Statistics Processing | 377 |
| Chapter 15 | Troubleshooting | 381 |
| | Troubleshooting Overload Conditions in the Mobile Network | 381 |
| | Troubleshooting Multilevel Overload Protection | 381 |
| | Responding to an Overload | 382 |
| | Monitoring GTP Signaling | 382 |
| | Troubleshooting Alarms, Logs, and Traps | 383 |
| | Troubleshooting Admission Control | 385 |
| | Monitoring AAA Metrics | 387 |
| Part 10 | Examples | |
| Chapter 16 | Example Configurations | 395 |
| | Example: Simple Unified Edge Configuration | 395 |
| | Example: Configuring MobileNext Broadband Gateway | 403 |
| | Example: Configuring MobileNext Broadband Gateway with Provider Edge Functionality | 431 |
| | Example: Configuring NAT | 440 |
| Part 11 | Complete Configuration Statement Hierarchy and Summary of Statements | |
| Chapter 17 | Configuration Statement Hierarchy | 447 |
| | [edit access] Hierarchy Level | 447 |
| | [edit access address-assignment] Hierarchy Level | 448 |
| | [edit class-of-service] Hierarchy Level | 449 |
| | [edit interfaces ams] Hierarchy Level | 449 |
| | [edit interfaces apfe] Hierarchy Level | 450 |
| | [edit interfaces mif] Hierarchy Level | 450 |
| | [edit routing-instance system] Hierarchy Level | 451 |
| | [edit services ip-reassembly] Hierarchy Level | 452 |
| | [edit services service-set] Hierarchy Level | 452 |
| | [edit unified-edge] Hierarchy Level | 452 |

| | | |
|-------------------|---|------------|
| | [edit unified-edge aaa] Hierarchy Level | 453 |
| | [edit unified-edge cos-cac] Hierarchy Level | 454 |
| | [edit unified-edge gateways] Hierarchy Level | 456 |
| | [edit unified-edge local-policies] Hierarchy Level | 465 |
| | [edit unified-edge mobile-options] Hierarchy Level | 466 |
| | [edit unified-edge resource-management] Hierarchy Level | 466 |
| Chapter 18 | AAA on the Broadband Gateway | 469 |
| | aaa | 470 |
| | accounting | 472 |
| | accounting-port | 473 |
| | accounting-secret | 473 |
| | address | 474 |
| | algorithm | 474 |
| | allow-dynamic-requests | 475 |
| | attributes | 476 |
| | authentication | 477 |
| | authentication-port | 477 |
| | dead-criteria-retries | 478 |
| | dynamic-requests-secret | 478 |
| | exclude | 479 |
| | ignore | 481 |
| | maximum-pending-reqs-limit | 481 |
| | mobile-profiles | 482 |
| | network-element | 484 |
| | network-element-group | 484 |
| | network-element-groups | 485 |
| | network-elements | 486 |
| | options | 487 |
| | radius (Access) | 488 |
| | radius | 490 |
| | retry | 492 |
| | revert-interval | 492 |
| | secret | 493 |
| | send-accounting-on | 493 |
| | servers | 494 |
| | source-interface | 495 |
| | stop-on-access-deny | 495 |
| | stop-on-failure | 496 |
| | timeout | 496 |
| | traceoptions | 497 |
| | traceoptions | 498 |
| | trigger | 499 |
| Chapter 19 | Address Assignment and DHCP Configuration Statements | 501 |
| | Address Assignment Configuration Statements | 502 |
| | address-assignment (MobileNext Broadband Gateway) | 502 |
| | ageing-window (Mobile Pools) | 503 |
| | default-pool (Mobile Pools) | 503 |
| | external-assigned (Mobile Pools) | 504 |

| | |
|---|-----|
| family (Mobile Pools) | 505 |
| mobile-pool-groups | 506 |
| mobile-pools | 507 |
| network (Mobile Pools) | 508 |
| pool-prefetch-threshold (Mobile Pools) | 509 |
| pool-snmp-trap-threshold (Mobile Pools) | 510 |
| range (Mobile Pools) | 511 |
| service-mode (Mobile Pools) | 512 |
| DHCP Configuration Statements | 513 |
| bind-interface | 513 |
| dead-server-retry-interval | 514 |
| dead-server-successive-retry-attempt | 515 |
| dhcp-proxy-client | 516 |
| dhcp-server-selection-algorithm | 517 |
| dhcpv4-profiles | 518 |
| dhcpv6-profiles | 519 |
| lease-time | 520 |
| pool-name | 520 |
| priority | 521 |
| retransmission-attempt | 522 |
| retransmission-interval | 523 |
| server | 524 |
| services | 525 |
| system | 526 |
| trace-options | 527 |

Chapter 20

| | |
|---|------------|
| Anchor Packet Forwarding Engine Redundancy and Aggregated Multiservices High Availability Configuration Statements | 529 |
| anchor-pfes | 529 |
| anchor-spics | 530 |
| anchoring-options (Aggregated Packet Forwarding Engine) | 531 |
| apfe-group-set (Aggregated Packet Forwarding Engine) | 532 |
| drop-member-traffic (Aggregated Multiservices) | 533 |
| enable-rejoin (Aggregated Multiservices) | 534 |
| family (Aggregated Multiservices) | 535 |
| high-availability-options (Aggregated Multiservices) | 536 |
| interface (Anchor Packet Forwarding Engine) | 537 |
| interface (Multiservices PIC) | 538 |
| interfaces (Aggregated Multiservices) | 539 |
| interfaces (Aggregated Packet Forwarding Engine) | 540 |
| load-balancing-options (Aggregated Multiservices) | 541 |
| many-to-one (Aggregated Multiservices) | 542 |
| member-failure-options (Aggregated Multiservices) | 543 |
| member-interface (Aggregated Multiservices) | 545 |
| primary-list (Aggregated Packet Forwarding Engine) | 546 |
| redistribute-all-traffic (Aggregated Multiservices) | 547 |
| rejoin-timeout (Aggregated Multiservices) | 548 |
| secondary (Aggregated Packet Forwarding Engine) | 549 |
| system | 550 |

| | | |
|-------------------|--|------------|
| | unit (Aggregated Multiservices) | 551 |
| | warm-standby (Aggregated Packet Forwarding Engine) | 552 |
| Chapter 21 | APN Configuration Statements | 553 |
| | APN Services Configuration Statements | 553 |
| | aaa (APN Address Assignment) | 553 |
| | aaa-override (APN Address Assignment) | 554 |
| | aaa-profile (APN) | 555 |
| | address-assignment (APN) | 556 |
| | allow-static-ip-address (APN Address Assignment) | 557 |
| | anonymous-user (APN) | 558 |
| | apn-data-type | 559 |
| | apn-services | 560 |
| | apn-type | 562 |
| | apns | 563 |
| | block-visitors | 565 |
| | charging (APN) | 566 |
| | default-profile (APN) | 567 |
| | description (APN) | 568 |
| | dhcp-proxy-client (APN Address Assignment) | 569 |
| | dhcpv4-proxy-client-profile (APN Address Assignment) | 570 |
| | dhcpv6-proxy-client-profile (APN Address Assignment) | 571 |
| | dns-server (APN) | 572 |
| | exclude-pools (APN Address Assignment) | 573 |
| | exclude-v6pools (APN Address Assignment) | 574 |
| | group (APN Address Assignment) | 575 |
| | home-profile (APN) | 576 |
| | idle-timeout (APN) | 577 |
| | idle-timeout-direction (APN) | 578 |
| | inet-pool (APN Address Assignment) | 579 |
| | inet6-pool (APN Address Assignment) | 580 |
| | inter-mobile-traffic (APN) | 581 |
| | local (APN Address Assignment) | 582 |
| | local-policy-profile (APN) | 583 |
| | logical-system (APN Address Assignment) | 584 |
| | maximum-bearers (APN) | 585 |
| | mobile-interface (APN) | 586 |
| | nbns-server (APN) | 587 |
| | no-address-verify (APN Address Assignment) | 588 |
| | p-cscf (APN) | 589 |
| | pool (APN Address Assignment) | 590 |
| | pool-name (APN Address Assignment) | 591 |
| | profile-name (APN Address Assignment) | 592 |
| | profile-selection-order (APN) | 593 |
| | restriction-value (APN) | 594 |
| | roamer-profile (APN) | 595 |
| | routing-instance (APN Address Assignment) | 596 |
| | selection-mode (APN) | 597 |
| | service-mode (APN) | 598 |

| | | |
|-------------------|---|------------|
| | service-selection-profile (APN) | 599 |
| | session-timeout (APN) | 600 |
| | verify-source-address (APN) | 601 |
| | visited-profile (APN) | 602 |
| | wait-accounting (APN) | 603 |
| | Service Selection Profiles Configuration Statements | 604 |
| | apn-name (Service Selection Profiles) | 604 |
| | charging-characteristics (Service Selection Profiles) | 605 |
| | from (Service Selection Profiles) | 606 |
| | imei (Service Selection Profiles) | 607 |
| | imsi (Service Selection Profiles) | 608 |
| | maximum-bearers (Service Selection Profiles) | 609 |
| | msisdn (Service Selection Profiles) | 610 |
| | pdn-type (Service Selection Profiles) | 611 |
| | peer (Service Selection Profiles) | 611 |
| | peer-routing-instance (Service Selection Profiles) | 612 |
| | profile (Service Selection Profiles) | 613 |
| | redirect-peer (Service Selection Profiles) | 614 |
| | service-selection-profiles | 615 |
| | term (Service Selection Profiles) | 616 |
| | then (Service Selection Profiles) | 617 |
| Chapter 22 | Charging Configuration Statements | 619 |
| | cdr-aggregation-limit | 619 |
| | cdr-profile | 620 |
| | cdr-profiles | 621 |
| | cdr-release | 622 |
| | cdrs-per-file | 623 |
| | charging | 624 |
| | charging-gateways | 627 |
| | charging-profiles | 628 |
| | container-limit | 629 |
| | default-rating-group | 629 |
| | default-service-id | 630 |
| | description | 631 |
| | destination-ipv4-address | 632 |
| | destination-port | 633 |
| | direction | 634 |
| | disable-replication | 635 |
| | disk-space-policy | 636 |
| | down-detect-time | 637 |
| | echo-interval | 638 |
| | enable-reduced-partial-cdrs | 639 |
| | exclude (Trigger Profiles) | 640 |
| | exclude-ie-options | 642 |
| | file-age | 646 |
| | file-creation-policy | 647 |
| | file-format | 648 |
| | file-name-private-extension | 649 |

| | |
|---|------------|
| file-size | 650 |
| gtp | 651 |
| header-type | 652 |
| local-persistent-storage-options | 653 |
| local-storage | 654 |
| mtu (Transport Profiles) | 655 |
| n3-requests | 656 |
| no-path-management | 657 |
| offline (Transport Profiles) | 658 |
| offline (Trigger profiles) | 659 |
| peer (GTP Prime) | 660 |
| peer (Peer Order) | 661 |
| peer-order | 662 |
| pending-queue-size | 663 |
| persistent-storage-order | 664 |
| profile-id | 665 |
| reconnect-time | 666 |
| service-mode (Charging Profiles) | 667 |
| service-mode (Transport Profiles) | 669 |
| sgsn-sgw-change-limit | 670 |
| source-interface | 671 |
| switch-back-time | 672 |
| t3-response | 673 |
| tariff-time-list | 674 |
| time-limit | 675 |
| traceoptions (Charging) | 676 |
| traceoptions (Persistent Storage) | 678 |
| transport-profile | 680 |
| transport-profiles | 681 |
| transport-protocol | 682 |
| trigger-profile | 683 |
| trigger-profiles | 684 |
| user-name | 685 |
| version | 686 |
| volume-limit | 687 |
| watermark-level-1 | 688 |
| watermark-level-2 | 689 |
| watermark-level-3 | 690 |
| world-readable | 691 |
| Chapter 23 Class of Service (CoS) Configuration Statements | 693 |
| aggregated-maximum-bit-rate | 693 |
| allocation-retention-priority | 694 |
| bandwidth-pools | 695 |
| bearer-load | 696 |
| classifier-profile | 697 |
| classifier-profiles | 698 |
| class-of-service | 699 |
| cos-cac | 700 |

| | |
|--|------------|
| cos-policy-profile | 702 |
| cos-policy-profiles | 703 |
| cpu | 704 |
| dl-bandwidth-pool | 705 |
| dscp-ipv6 | 705 |
| dscp-ipv6 (Ingress) | 706 |
| dscp | 706 |
| dscp (Ingress) | 707 |
| exceed-action | 707 |
| guaranteed-bit-rate | 708 |
| high | 709 |
| inet-precedence | 709 |
| inet-precedence (Ingress) | 710 |
| ingress-rewrite-rules | 710 |
| interfaces | 711 |
| local-policies | 712 |
| local-policy-profile (MobileNext Broadband Gateway) | 713 |
| low | 714 |
| maximum-bearers (MobileNext Broadband Gateway) | 715 |
| maximum-bit-rate | 716 |
| memory | 717 |
| mif | 718 |
| preemption (MobileNext Broadband Gateway) | 719 |
| qos-class-identifier | 720 |
| resource-threshold-profiles | 721 |
| resource-threshold-profile | 722 |
| rewrite-rules | 723 |
| roamer-classifier-profile | 723 |
| roamer-cos-policy-profile | 724 |
| system-load | 725 |
| traffic-class-classifier-profiles | 726 |
| traffic-class-cos-policy-profiles | 727 |
| ul-bandwidth-pool | 728 |
| violate-action | 728 |
| visitor-classifier-profile | 729 |
| visitor-cos-policy-profile | 729 |
| Chapter 24 | |
| Exception Handling Configuration Statements | 731 |
| current-hop-limit (IPv6 Router Advertisement) | 731 |
| disable (IPv6 Router Advertisement) | 732 |
| error-indication-interval | 732 |
| ip-reassembly | 733 |
| ip-reassembly-profile | 734 |
| ipv6-router-advertisement (MobileNext Broadband Gateway) | 735 |
| max-reassembly-pending-packets (IP Reassembly) | 736 |
| maximum-advertisement-interval (IPv6 Router Advertisement) | 737 |
| maximum-initial-advertisement-interval (IPv6 Router Advertisement) | 738 |
| maximum-initial-advertisements (IPv6 Router Advertisement) | 739 |
| minimum-advertisement-interval (IPv6 Router Advertisement) | 740 |

| | | |
|-------------------|--|------------|
| | reachable-time (IPv6 Router Advertisement) | 741 |
| | retransmission-timer (IPv6 Router Advertisement) | 742 |
| | router-lifetime (IPv6 Router Advertisement) | 743 |
| | software-datapath | 744 |
| | timeout (IP Reassembly) | 745 |
| | traceoptions (Exception Handling) | 746 |
| Chapter 25 | Gateway Maintenance Mode Configuration Statement | 749 |
| | service-mode (Gateways) | 749 |
| Chapter 26 | GTP Configuration Statements | 751 |
| | control | 751 |
| | data | 752 |
| | dscp-code-point | 752 |
| | echo-interval | 753 |
| | echo-n3-requests | 753 |
| | echo-t3-response | 754 |
| | error-indication-interval | 754 |
| | forwarding-class | 755 |
| | gn | 756 |
| | gp | 757 |
| | gtp | 758 |
| | interface | 761 |
| | v4-address | 762 |
| | n3-requests | 762 |
| | path-management | 763 |
| | peer | 763 |
| | peer-groups | 764 |
| | peer-history | 765 |
| | routing-instance | 765 |
| | s5 | 766 |
| | s8 | 767 |
| | sequence-number-length | 768 |
| | t3-response | 768 |
| | traceoptions | 769 |
| Chapter 27 | Service Applications Configuration Statements | 771 |
| | egress-key (Aggregated Multiservices) | 771 |
| | hash-keys (Aggregated Multiservices) | 772 |
| | ingress-key (Aggregated Multiservices) | 773 |
| | interface-service (Aggregated Multiservices) | 774 |
| | load-balancing-options (Aggregated Multiservices) | 775 |
| | service-set (Aggregated Multiservices) | 776 |
| Chapter 28 | System Architecture and Gateway Traceoptions Configuration Statements | 779 |
| | System Architecture Configuration Statements | 779 |
| | call-rate-statistics | 779 |
| | family (Mobile Interface) | 780 |
| | filter (Mobile Interface) | 780 |
| | forwarding-packages | 781 |

| | |
|--|-----|
| ggsn-pgw | 782 |
| history (Call-Rate Statistics) | 782 |
| home-plmn | 783 |
| input (Mobile Interface) | 783 |
| interface | 784 |
| interfaces (Mobile Interface) | 785 |
| interval (Call-Rate Statistics) | 786 |
| mcc | 787 |
| mnc | 788 |
| mobility | 789 |
| mtu (Mobile Interface) | 790 |
| output (Mobile Interface) | 790 |
| unit (Mobile Interface) | 791 |
| Gateway Traceoptions Configuration Statements | 792 |
| client (Resource Management) | 792 |
| mobile-options | 793 |
| resource-management (MobileNext Broadband Gateway) | 794 |
| server (Resource Management) | 795 |
| traceoptions (MobileNext Broadband Gateway) | 796 |
| traceoptions (Mobile Options) | 798 |
| traceoptions (Resource Management Client) | 800 |
| traceoptions (Resource Management Server) | 803 |

Part 12

Chapter 29

Command Reference

AAA Operational Commands 809

| | |
|---|-----|
| clear unified-edge ggsn-pgw aaa radius statistics | 810 |
| clear unified-edge ggsn-pgw aaa statistics | 811 |
| clear unified-edge ggsn-pgw address-assignment pool-name | 812 |
| clear unified-edge ggsn-pgw address-assignment statistics | 813 |
| show unified-edge ggsn-pgw aaa network element-group status | 814 |
| show unified-edge ggsn-pgw aaa network element status | 816 |
| show unified-edge ggsn-pgw aaa radius statistics | 817 |
| show unified-edge ggsn-pgw aaa statistics accounting | 819 |
| show unified-edge ggsn-pgw aaa statistics authentication | 821 |
| show unified-edge ggsn-pgw aaa statistics dynamic-requests | 823 |
| show unified-edge ggsn-pgw address-assignment group | 825 |
| show unified-edge ggsn-pgw address-assignment pool name | 827 |
| show unified-edge ggsn-pgw address-assignment service-mode | 829 |
| show unified-edge ggsn-pgw address-assignment statistics | 831 |

Chapter 30

Anchor Packet Forwarding Engine Redundancy and Aggregated Multiservices High Availability Operational Commands 833

| | |
|--|-----|
| request interface load-balancing revert (Aggregated Multiservices) | 834 |
| request interface load-balancing switchover (Aggregated Multiservices) | 835 |
| show interfaces anchor-group (Aggregated Packet Forwarding Engine) | 836 |
| show interfaces load-balancing (Aggregated Multiservices) | 839 |
| show unified-edge ggsn-pgw system interfaces | 842 |

| | | |
|-------------------|--|------------|
| Chapter 31 | APN and Related Operational Commands | 845 |
| | clear unified-edge ggsn-pgw statistics | 846 |
| | clear unified-edge ggsn-pgw subscribers | 847 |
| | clear unified-edge ggsn-pgw subscribers charging | 849 |
| | clear unified-edge ggsn-pgw subscribers peer | 850 |
| | show unified-edge ggsn-pgw apn service-mode | 851 |
| | show unified-edge ggsn-pgw apn statistics | 854 |
| | show unified-edge ggsn-pgw gateway service-mode | 858 |
| | show unified-edge ggsn-pgw statistics | 860 |
| | show unified-edge ggsn-pgw status | 862 |
| | show unified-edge ggsn-pgw subscribers | 865 |
| Chapter 32 | Charging Operational Commands | 875 |
| | clear unified-edge ggsn-pgw charging cdr | 876 |
| | clear unified-edge ggsn-pgw charging cdr wfa | 877 |
| | clear unified-edge ggsn-pgw charging local-persistent-storage statistics | 878 |
| | clear unified-edge ggsn-pgw charging path statistics | 879 |
| | clear unified-edge ggsn-pgw charging transfer statistics | 880 |
| | request system storage unified-edge charging media start | 881 |
| | request system storage unified-edge charging media stop | 882 |
| | request system storage unified-edge media eject | 883 |
| | request system storage unified-edge media prepare | 884 |
| | show unified-edge ggsn-pgw charging local-persistent-storage statistics | 885 |
| | show unified-edge ggsn-pgw charging path statistics | 890 |
| | show unified-edge ggsn-pgw charging path status | 930 |
| | show unified-edge ggsn-pgw charging service-mode | 932 |
| | show unified-edge ggsn-pgw charging transfer statistics | 935 |
| | show unified-edge ggsn-pgw charging transfer status | 946 |
| | show unified-edge ggsn-pgw charging trigger-profile | 954 |
| Chapter 33 | Class of Service (CoS) Operational Commands | 957 |
| | show unified-edge ggsn-pgw qos statistics | 958 |
| | show unified-edge ggsn-pgw status preemption-list | 960 |
| Chapter 34 | Exception Handling Operational Commands | 963 |
| | clear unified-edge ggsn-pgw exception-handling statistics | 964 |
| | clear unified-edge ggsn-pgw ip-reassembly statistics | 965 |
| | show unified-edge ggsn-pgw exception-handling statistics | 966 |
| | show unified-edge ggsn-pgw ip-reassembly statistics | 970 |
| Chapter 35 | GPRS Tunneling Protocol (GTP) Operational Commands | 973 |
| | show unified-edge ggsn-pgw gtp statistics | 974 |
| | show unified-edge ggsn-pgw gtp peer | 976 |
| | clear unified-edge ggsn-pgw gtp statistics | 978 |
| | clear unified-edge ggsn-pgw gtp peer statistics | 979 |
| Chapter 36 | Service Applications Operational Commands | 981 |
| | show services flows (Aggregated Multiservices) | 982 |
| | show services nat mappings app | 986 |
| | show services nat mappings eim | 988 |
| | show services nat mappings summary | 990 |

| | | |
|-------------------|---|-------------|
| | show services nat pool (Aggregated Multiservices) | 991 |
| | show services nat statistics | 994 |
| | show services service-sets summary | 1003 |
| | show services sessions (Aggregated Multiservices) | 1005 |
| Chapter 37 | System Architecture Operational Commands | 1013 |
| | show unified-edge ggsn-pgw call-rate statistics | 1014 |
| | show unified-edge ggsn-pgw resource-manager clients | 1016 |
| Part 13 | Index | |
| | Index | 1021 |
| | Index of Statements and Commands | 1039 |

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 | 5 |
| | Figure 3: Broadband Gateway Uplink User Packet Flow | 7 |
| | Figure 4: Broadband Gateway Downlink User Packet Flow | 8 |
| Chapter 2 | Network Architecture | 21 |
| | Figure 5: 3G Mobile Network Architecture | 23 |
| | Figure 6: 4G/LTE Mobile Network Basic Components | 24 |
| | Figure 7: Packet Data Network Gateway Functions | 25 |
| | Figure 8: Major Components of the Evolved Packet Core | 27 |
| | Figure 9: APNs and the P-GW | 29 |
| | Figure 10: Bearers, Gateways, and Packet Networks | 30 |
| | Figure 11: The GGSN in a 3G Network | 31 |
| | Figure 12: LTE Network Deployment Scenario | 33 |
| Part 2 | System Configuration | |
| Chapter 3 | Configuring Mobility on MX 3D Devices | 37 |
| | Figure 13: Session DPCs and Interfaces on the Broadband Gateway | 38 |
| | Figure 14: Upstream GTP-U Traffic | 46 |
| | Figure 15: Downstream GTP-U Traffic | 46 |
| Chapter 4 | Configuring Redundancy on MX 3D Devices | 49 |
| | Figure 16: Redundancy Available on the Broadband Gateway | 50 |
| | Figure 17: Control Plane Anchor Operation Before Failure | 56 |
| | Figure 18: Control Plane Anchor Operation After Failure | 57 |
| | Figure 19: Pre- and Post-Failure PFE Datapaths | 57 |
| | Figure 20: Redundancy Example for the Broadband Gateway | 59 |
| Chapter 5 | Configuring Mobile Edge Exception Handling | 63 |
| | Figure 21: GTP-C Handling | 64 |
| Part 3 | APN Configuration | |
| Chapter 6 | Configuring APNs | 79 |
| | Figure 22: APNs and P-GWs in the 4G Architecture | 80 |
| | Figure 23: APNs Connect Mobile Devices to IP Networks Through a P-GW | 101 |

| | | |
|-------------------|---|------------|
| Part 5 | GPRS Tunneling Protocol (GTP) Configuration | |
| Chapter 9 | Configuring GTP | 173 |
| | Figure 24: GTP Versions Supported on a MobileNext Broadband Gateway | 174 |
| | Figure 25: GTP-C Versions Supported for 3G/4G Network Interfaces | 174 |
| | Figure 26: Successful Echo-Request Sequence for Path Management | 178 |
| | Figure 27: Failed Echo-Request Sequence for Path Management | 179 |
| | Figure 28: Successful Create Request Sequence for Tunnel Management | 181 |
| | Figure 29: Successful Update/Delete Request Sequence for Tunnel Management | 182 |
| | Figure 30: Failed Update/Delete Request Sequence for Tunnel Management | 183 |
| | Figure 31: GTP-C Performs Signaling Between the Serving Gateway and Packet Data Network Gateway | 185 |
| Part 6 | Charging Configuration | |
| Chapter 10 | Charging Overview | 211 |
| | Figure 32: Simple Charging Topology | 212 |
| Part 7 | Quality of Service Configuration | |
| Chapter 12 | Configuring Quality of Service | 239 |
| | Figure 33: Key QoS Parameters for PDP Context Requests | 242 |
| | Figure 34: Key QoS Parameters for 4G Default Bearer Requests | 243 |
| | Figure 35: QoS Negotiation Behavior for PDP Contexts with NQN and Upgrade Flags | 252 |

List of Tables

| | | |
|------------------|---|-------------|
| | About This Guide | xxix |
| | Table 1: Notice Icons | xxxiii |
| | Table 2: Text and Syntax Conventions | xxxiii |
| Part 1 | Overview | |
| Chapter 1 | System Architecture | 3 |
| | Table 3: General Gateway Trace Flags | 14 |
| | Table 4: Trace Levels | 15 |
| | Table 5: Mobile Options Trace Flags | 16 |
| | Table 6: Trace Levels | 16 |
| | Table 7: Resource Management Server Trace Flags | 18 |
| | Table 8: Resource Management Client Trace Flags | 19 |
| | Table 9: Trace Levels | 19 |
| Part 2 | System Configuration | |
| Chapter 5 | Configuring Mobile Edge Exception Handling | 63 |
| | Table 10: Trace Flags | 70 |
| | Table 11: Trace Levels | 71 |
| Part 3 | APN Configuration | |
| Chapter 6 | Configuring APNs | 79 |
| | Table 12: APN Restriction Values | 88 |
| Part 4 | Authorization and Addressing Configuration | |
| Chapter 7 | Configuring AAA | 107 |
| | Table 13: RADIUS IETF Attributes Supported in Access-Request Messages | 115 |
| | Table 14: 3GPP VSAs Supported in Access-Request Messages | 117 |
| | Table 15: RADIUS IETF Attributes Supported in Access-Accept Messages | 120 |
| | Table 16: 3GPP VSAs Supported in Access-Accept Messages | 121 |
| | Table 17: Juniper VSAs Supported in Access-Accept Messages | 122 |
| | Table 18: RADIUS IETF Attributes Supported in Accounting Start Messages | 123 |
| | Table 19: 3GPP VSAs Supported in Accounting Start Messages | 124 |
| | Table 20: RADIUS IETF Attributes Supported in Accounting Interim-Update Messages | 127 |
| | Table 21: 3GPP VSAs Supported in Accounting Interim-Update Messages | 129 |
| | Table 22: RADIUS IETF Attributes Supported in Accounting Stop Messages | 131 |
| | Table 23: 3GPP VSAs Supported in Accounting Stop Messages | 133 |

| | | |
|-------------------|---|------------|
| | Table 24: RADIUS IETF Attributes Supported in Accounting On Messages | 136 |
| | Table 25: RADIUS IETF Attributes Supported in Disconnect Request Messages | 136 |
| | Table 26: 3GPP VSAs Supported in Disconnect Request Messages | 137 |
| | Table 27: RADIUS IETF Attributes Supported in CoA Messages | 138 |
| | Table 28: 3GPP VSAs Supported in CoA Messages | 138 |
| | Table 29: Events You Can Exclude from Triggering Interim-Update Messages . . | 145 |
| | Table 30: RADIUS Attributes the Broadband Gateway Can Ignore in Accept-Accept Messages | 147 |
| | Table 31: RADIUS Attributes the Broadband Gateway Can Exclude from RADIUS Messages | 147 |
| | Table 32: 3GPP VSAs That Can Be Excluded from RADIUS Messages | 148 |
| Part 5 | GPRS Tunneling Protocol (GTP) Configuration | |
| Chapter 9 | Configuring GTP | 173 |
| | Table 33: Trace Flags | 207 |
| | Table 34: Trace Levels | 207 |
| Part 7 | Quality of Service Configuration | |
| Chapter 12 | Configuring Quality of Service | 239 |
| | Table 35: Traffic Classes for a 3G Network | 241 |
| | Table 36: QoS Class Identifier for a 4G Network | 242 |
| Part 10 | Examples | |
| Chapter 16 | Example Configurations | 395 |
| | Table 37: Unified Edge — Simple Configuration | 396 |
| | Table 38: Components of the Broadband Gateway | 403 |
| | Table 39: Components of the Broadband Gateway | 432 |
| Part 11 | Complete Configuration Statement Hierarchy and Summary of Statements | |
| Chapter 20 | Anchor Packet Forwarding Engine Redundancy and Aggregated Multiservices High Availability Configuration Statements | 529 |
| | Table 40: Behavior of Member Interface After One Multiservices PIC Fails . . . | 543 |
| | Table 41: Behavior of Member Interface After Two Multiservices PICs Fail . . . | 544 |
| Chapter 21 | APN Configuration Statements | 553 |
| | Table 42: Valid Restriction Values for APNs | 594 |
| | Table 43: Selection Mode Values | 597 |
| Chapter 22 | Charging Configuration Statements | 619 |
| | Table 44: Triggers and corresponding IEs | 640 |
| Chapter 27 | Service Applications Configuration Statements | 771 |
| | Table 45: Hash Keys Supported for AMS for Service Applications | 772 |

| | | |
|-------------------|---|------------|
| Part 12 | Command Reference | |
| Chapter 29 | AAA Operational Commands | 809 |
| | Table 46: show unified-edge ggsn-pgw aaa network element-group status Output Fields | 814 |
| | Table 47: show unified-edge ggsn-pgw aaa network element status Output Fields | 816 |
| | Table 48: show unified-edge ggsn-pgw aaa radius statistics Output Fields | 817 |
| | Table 49: show unified-edge ggsn-pgw aaa statistics accounting Output Fields | 819 |
| | Table 50: show unified-edge ggsn-pgw aaa statistics authentication Output Fields | 821 |
| | Table 51: show unified-edge ggsn-pgw aaa statistics dynamic-requests Output Fields | 823 |
| | Table 52: show unified-edge ggsn-pgw address-assignment-group Output Fields | 825 |
| | Table 53: show unified-edge ggsn-pgw address-assignment pool Output Fields | 827 |
| | Table 54: show unified-edge ggsn-pgw address-assignment service-mode Output Fields | 829 |
| | Table 55: show unified-edge ggsn-pgw address-assignment statistics Output Fields | 831 |
| Chapter 30 | Anchor Packet Forwarding Engine Redundancy and Aggregated Multiservices High Availability Operational Commands | 833 |
| | Table 56: show interfaces anchor-group | 836 |
| | Table 57: show interfaces load-balancing Output Fields | 839 |
| | Table 58: show unified-edge ggsn-pgw system interfaces | 842 |
| Chapter 31 | APN and Related Operational Commands | 845 |
| | Table 59: show unified-edge ggsn-pgw apn service-mode Output Fields | 851 |
| | Table 60: show unified-edge ggsn-pgw apn statistics Output Fields | 854 |
| | Table 61: show unified-edge ggsn-pgw gateway service-mode Output Fields | 858 |
| | Table 62: show unified-edge ggsn-pgw statistics Output Fields | 860 |
| | Table 63: show unified-edge ggsn-pgw status Output Fields | 863 |
| | Table 64: show unified-edge ggsn-pgw subscribers Output Fields | 866 |
| Chapter 32 | Charging Operational Commands | 875 |
| | Table 65: show unified-edge ggsn-pgw charging local-persistent-storage statistics Output Fields | 885 |
| | Table 66: show unified-edge ggsn-pgw charging path statistics Output Fields | 890 |
| | Table 67: show unified-edge ggsn-pgw charging path status Output Fields | 930 |
| | Table 68: show unified-edge ggsn-pgw charging service-mode gateway gateway-name Output Fields | 932 |
| | Table 69: show unified-edge ggsn-pgw charging transfer statistics Output Fields | 935 |
| | Table 70: show unified-edge ggsn-pgw charging transfer status Output Fields | 946 |
| | Table 71: show unified-edge ggsn-pgw charging trigger-profile Output Fields | 954 |

| | | |
|-------------------|---|-------------|
| Chapter 33 | Class of Service (CoS) Operational Commands | 957 |
| | Table 72: show unified-edge ggsn-pgw qos statistics Output Fields | 958 |
| | Table 73: show unified-edge ggsn-pgw status preemption-list Output Fields . . | 960 |
| Chapter 34 | Exception Handling Operational Commands | 963 |
| | Table 74: show unified-edge ggsn-pgw exception-handling statistics Output Fields | 967 |
| | Table 75: show unified-edge ggsn-pgw ip-reassembly statistics Output Fields | 970 |
| Chapter 35 | GPRS Tunneling Protocol (GTP) Operational Commands | 973 |
| | Table 76: show unified-edge ggsn-pgw gtp statistics Output Fields | 974 |
| | Table 77: show unified-edge ggsn-pgw gtp statistics Output Fields | 976 |
| Chapter 36 | Service Applications Operational Commands | 981 |
| | Table 78: show services flows Output Fields | 984 |
| | Table 79: show services nat mappings app Output Fields | 986 |
| | Table 80: show services nat mappings eim Output Fields | 988 |
| | Table 81: show services nat mappings summary Output Fields | 990 |
| | Table 82: show services nat pool Output Fields | 991 |
| | Table 83: show services nat statistics Output Fields | 994 |
| | Table 84: show services service-sets summary Output Fields | 1003 |
| | Table 85: show services sessions Output Fields | 1007 |
| Chapter 37 | System Architecture Operational Commands | 1013 |
| | Table 86: show unified-edge ggsn-pgw call-rate statistics Output Fields | 1014 |
| | Table 87: show unified-edge gateways ggsn-pgw resource-manager clients Output Fields | 1016 |

About This Guide

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

- [Junos Documentation and Release Notes on page xxix](#)
- [Objectives on page xxx](#)
- [Audience on page xxx](#)
- [Supported Platforms on page xxx](#)
- [Using the Indexes on page xxxi](#)
- [Using the Examples in This Manual on page xxxi](#)
- [Documentation Conventions on page xxxii](#)
- [Documentation Feedback on page xxxiv](#)
- [Requesting Technical Support on page xxxiv](#)

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 xxxiii 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 xxxiii 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: [edit] root@# set system domain-name <i>domain-name</i> |
| 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 [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE. |
| < > (angle brackets) | Enclose optional keywords or variables. | <code>stub <default-metric metric>;</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 string2 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 [community-ids] |
| Indentation and braces ({ }) | Identify a level in the configuration hierarchy. | [edit] routing-options { static { route default { nexthop address; 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 21](#)

CHAPTER 1

System Architecture

- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Overview of Broadband Gateway System Control Packet Flow on page 5](#)
- [Overview of Broadband Gateway Uplink Payload Packet Flow on page 7](#)
- [Overview of Broadband Gateway Downlink Payload Packet Flow on page 8](#)
- [Overview of Broadband Gateway as GGSN or P-GW on page 9](#)
- [Understanding Mobile User Types on page 10](#)
- [Configuring Broadband Gateway Home PLMNs and Gateways on page 10](#)
- [Configuring Broadband Gateway Local Policies Application on page 11](#)
- [Configuring Broadband Gateway Call Rate Statistics on page 13](#)
- [Verifying the Gateway Configuration on page 13](#)
- [Configuring General Gateway Trace Options on page 14](#)
- [Configuring Mobile Options Trace Options on page 16](#)
- [Configuring Resource Manager Trace Options on page 18](#)

Overview of Broadband Gateway System Architecture

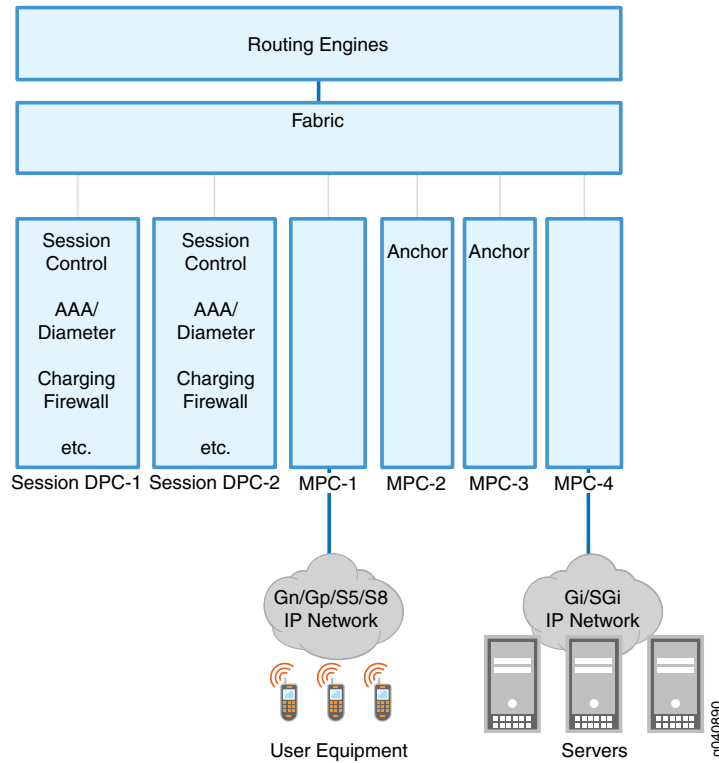
The distinctive architecture of the MobileNext Broadband Gateway allows the functions of the gateway GPRS support node (GGSN) or Packet Data Network Gateway (P-GW) in 2G, 3G, and 4G architectures to combine with a typical provider edge (PE) router. Service chaining helps with scaling and lets the broadband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

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

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

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

Figure 1: The Broadband Gateway System Architecture



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

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

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

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



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

Related Documentation

- [Overview of Broadband Gateway System Control Packet Flow on page 5](#)
- [Overview of Broadband Gateway Uplink Payload Packet Flow on page 7](#)
- [Overview of Broadband Gateway Downlink Payload Packet Flow on page 8](#)
- [Overview of Broadband Gateway as GGSN or P-GW on page 9](#)

Overview of Broadband Gateway System Control Packet Flow

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

Figure 2: Broadband Gateway GTP Signaling Packet Flow

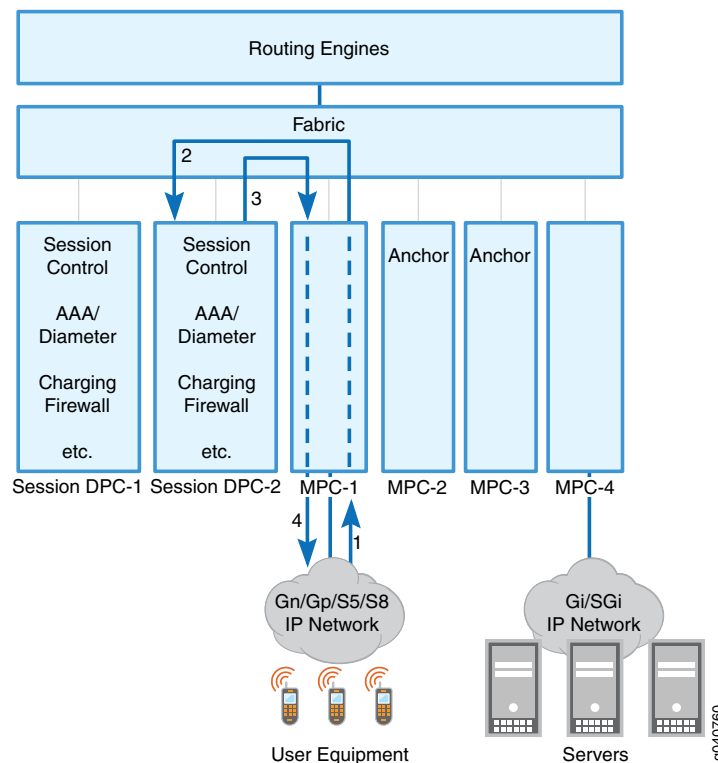


Figure 2 on page 5 shows the four steps that GTP-C signaling packets take through the broadband gateway:

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

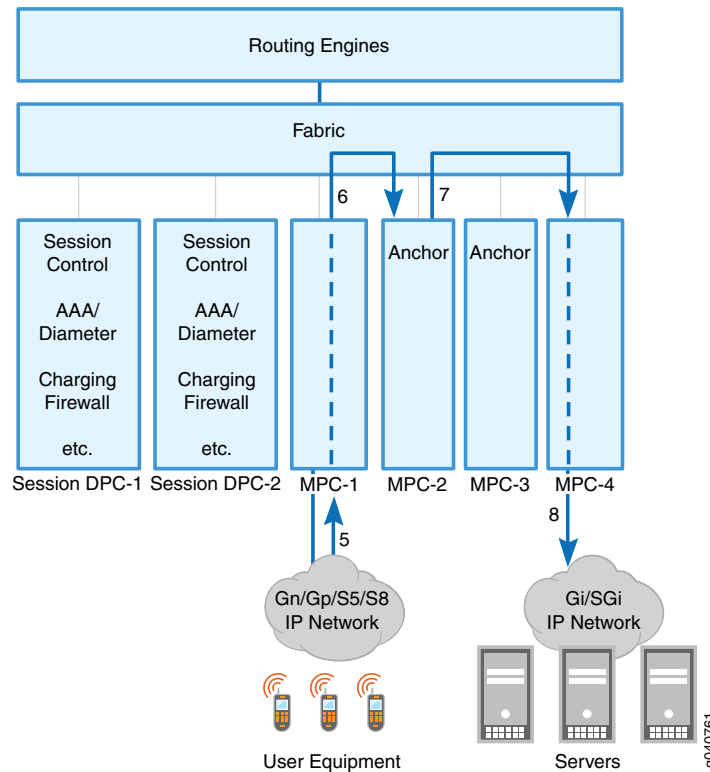
**Related
Documentation**

- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Overview of Broadband Gateway Uplink Payload Packet Flow on page 7](#)
- [Overview of Broadband Gateway Downlink Payload Packet Flow on page 8](#)
- [Overview of Broadband Gateway as GGSN or P-GW on page 9](#)

Overview of Broadband Gateway Uplink Payload Packet Flow

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

Figure 3: Broadband Gateway Uplink User Packet Flow



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

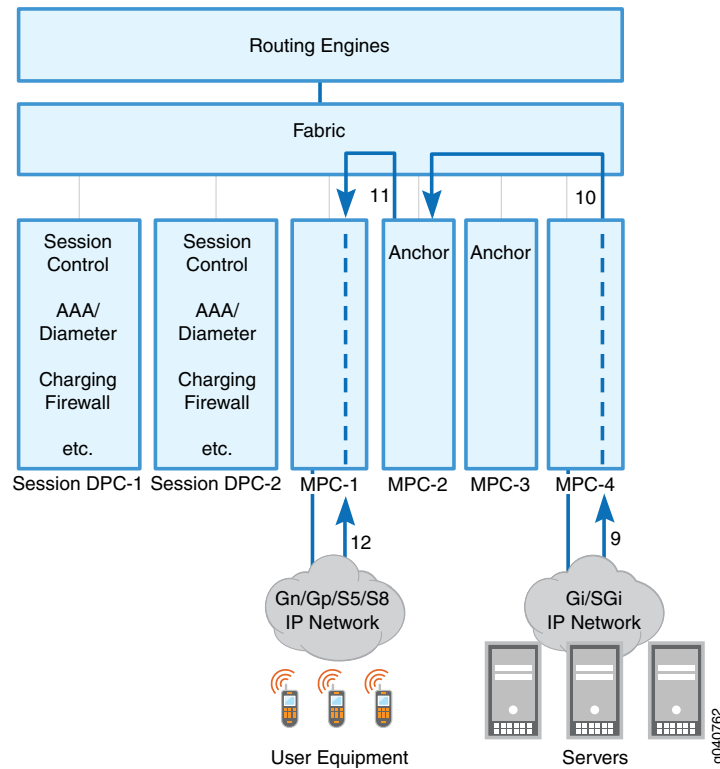
5. An attached user equipment device sends an uplink payload GTP-U packet to a mobile interface on the broadband gateway.
6. The interface MPC sends the GTP-U packet to the interface MPC chosen during the control phase to anchor the user session data flow. The anchor MPC performs all subscriber-specific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

- Related Documentation**
- [Overview of Broadband Gateway System Architecture on page 3](#)
 - [Overview of Broadband Gateway System Control Packet Flow on page 5](#)
 - [Overview of Broadband Gateway Downlink Payload Packet Flow on page 8](#)
 - [Overview of Broadband Gateway as GGSN or P-GW on page 9](#)

Overview of Broadband Gateway Downlink Payload Packet Flow

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

Figure 4: Broadband Gateway Downlink User Packet Flow



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

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

Related Documentation

- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Overview of Broadband Gateway System Control Packet Flow on page 5](#)
- [Overview of Broadband Gateway Uplink Payload Packet Flow on page 7](#)
- [Overview of Broadband Gateway as GGSN or P-GW on page 9](#)

Overview of Broadband Gateway as GGSN or P-GW

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

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

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

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

- Mobile subscriber authentication with RADIUS.

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

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

**Related
Documentation**

- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Configuring Broadband Gateway Home PLMNs and Gateways on page 10](#)

Understanding Mobile User Types

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

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

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

**Related
Documentation**

- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Configuring Broadband Gateway Home PLMNs and Gateways on page 10](#)
- [Configuring Broadband Gateway Local Policies Application on page 11](#)

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 10](#)
- [Configuring Broadband Gateway Local Policies Application on page 11](#)
- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Configuring General Gateway Trace Options on page 14](#)
- [Configuring Mobile Options Trace Options on page 16](#)
- [Configuring Resource Manager Trace Options on page 18](#)

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 10](#)
- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Configuring General Gateway Trace Options on page 14](#)
- [Configuring Mobile Options Trace Options on page 16](#)
- [Configuring Resource Manager Trace Options on page 18](#)

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 10](#)
- [Configuring General Gateway Trace Options on page 14](#)
- [Configuring Mobile Options Trace Options on page 16](#)
- [Configuring Resource Manager Trace Options on page 18](#)

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 10](#)
- [Configuring Broadband Gateway Local Policies Application on page 11](#)
- [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 14](#) 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 |
|----------------------|---|
| <code>all</code> | Trace everything. |
| <code>bulkjob</code> | Trace resources. |
| <code>config</code> | Trace configuration events. |
| <code>cos-cac</code> | Trace CoS and CAC events. |
| <code>ctext</code> | Trace user equipment, PDN, or bearer context events. |
| <code>fsm</code> | Trace FSM events. |
| <code>gtpu</code> | Trace GTP-U events. |
| <code>ha</code> | Trace high availability events. |
| <code>init</code> | Trace events related to protocol daemon initialization. |
| <code>pfem</code> | Trace PFE manager events. |

Table 3: General Gateway Trace Flags (*continued*)

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

To configure tracing options for general gateway events:

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

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

2. Configure the filename for the trace file.

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

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

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



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

4. Configure the tracing flag.

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



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

5. Configure the tracing level.

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

6. View the trace file.

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

Related Documentation

- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Configuring Broadband Gateway Home PLMNs and Gateways on page 10](#)
- [Configuring Broadband Gateway Local Policies Application on page 11](#)
- [Configuring Mobile Options Trace Options on page 16](#)
- [Configuring Resource Manager Trace Options on page 18](#)

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 16](#) 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 16](#) describes the levels you can include.

Table 6: Trace Levels

| Level | Description |
|--------------|-------------------------------|
| all | Match all levels. |
| error | Match error conditions. |
| info | Match informational messages. |

Table 6: Trace Levels (*continued*)

| | |
|---------|--|
| 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 3](#)
- [Configuring Broadband Gateway Home PLMNs and Gateways on page 10](#)
- [Configuring Broadband Gateway Local Policies Application on page 11](#)
- [Configuring General Gateway Trace Options on page 14](#)

- [Configuring Resource Manager Trace Options on page 18](#)

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 18](#) 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 19 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 |
|------------------------------|-------------------------------|
| <code>all</code> | Trace everything. |
| <code>communication</code> | Trace IPC code. |
| <code>info-tables</code> | Trace information table code. |
| <code>infra</code> | Trace FSM and Infra code. |
| <code>memory</code> | Trace memory management code. |
| <code>redundancy</code> | Trace GRES code. |
| <code>resource-tables</code> | Trace resource table code. |

Table 9 on page 19 describes the levels you can include.

Table 9: Trace Levels

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

To configure tracing options for resource management operations:

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

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

2. Configure the filename for the trace file.

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

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

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



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

4. Configure the tracing flag.

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



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

5. Configure the tracing level.

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

6. View the trace file.

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

**Related
Documentation**

- [Overview of Broadband Gateway System Architecture on page 3](#)
- [Configuring Broadband Gateway Home PLMNs and Gateways on page 10](#)
- [Configuring Broadband Gateway Local Policies Application on page 11](#)
- [Configuring General Gateway Trace Options on page 14](#)
- [Configuring Mobile Options Trace Options on page 16](#)

CHAPTER 2

Network Architecture

- [Overview of Mobile Networks on page 21](#)
- [Overview of 3G Mobile Networks and the MobileNext Broadband Gateway on page 22](#)
- [Overview of GGSN and P-GW on page 24](#)
- [Overview of Packet Data Network Gateway Functions on page 25](#)
- [Overview of the Evolved Packet Core on page 26](#)
- [Overview of APNs on page 28](#)
- [Overview of PDP Contexts and Bearers on page 30](#)
- [Overview of GGSN and Broadband Gateway Deployment on page 31](#)
- [Overview of 4G/LTE and Broadband Gateway Deployment on page 32](#)
- [Overview of IPv6 and the Broadband Gateway on page 34](#)

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**

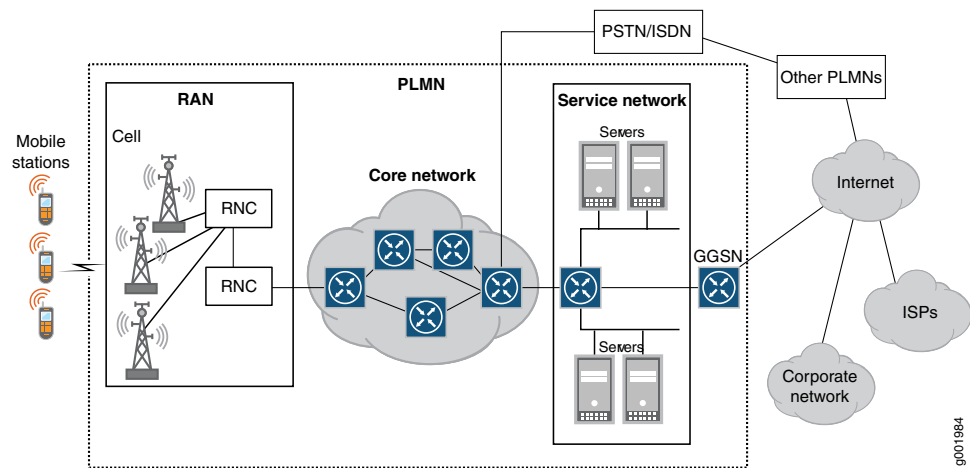
- [Overview of Packet Data Network Gateway Functions on page 25](#)
- [Overview of APNs on page 28](#)
- [Overview of PDP Contexts and Bearers on page 30](#)
- [Overview of IPv6 and the Broadband Gateway on page 34](#)

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 5 on page 23](#) 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 5: 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 (BTSs) or NodeBs in 3G. In some versions, there are also Radio Network Controllers (RNCs) that link to the BTSs 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 5 on page 23](#). 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 5 on page 23](#)) 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 Packet Data Network Gateway Functions on page 25](#)
- [Overview of APNs on page 28](#)
- [Overview of PDP Contexts and Bearers on page 30](#)

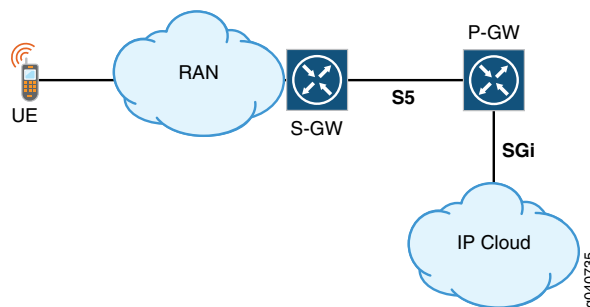
- [Overview of IPv6 and the Broadband Gateway on page 34](#)

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 6 on page 24](#) shows the major components and interfaces of a mobile network based on 4G/LTE standards.

Figure 6: 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 Packet Data Network Gateway Functions on page 25](#)
- [Overview of APNs on page 28](#)
- [Overview of PDP Contexts and Bearers on page 30](#)
- [Overview of IPv6 and the Broadband Gateway on page 34](#)

Overview of Packet Data Network Gateway Functions

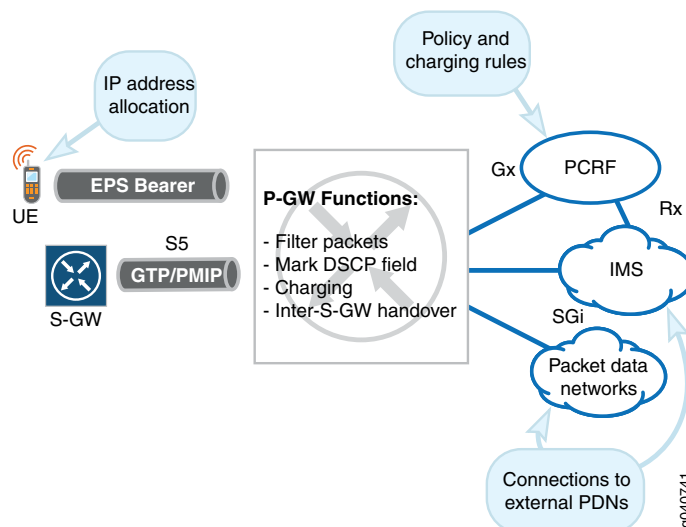
In a mobile network, a major function of the Packet Data Network Gateway (P-GW) is to allocate IP addresses to the user equipment during default bearer setup. The user equipment can still connect to multiple packet networks through multiple P-GWs, and also to older, non-3GPP-compliant IP networks.



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 7: 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 7 on page 25](#) 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**

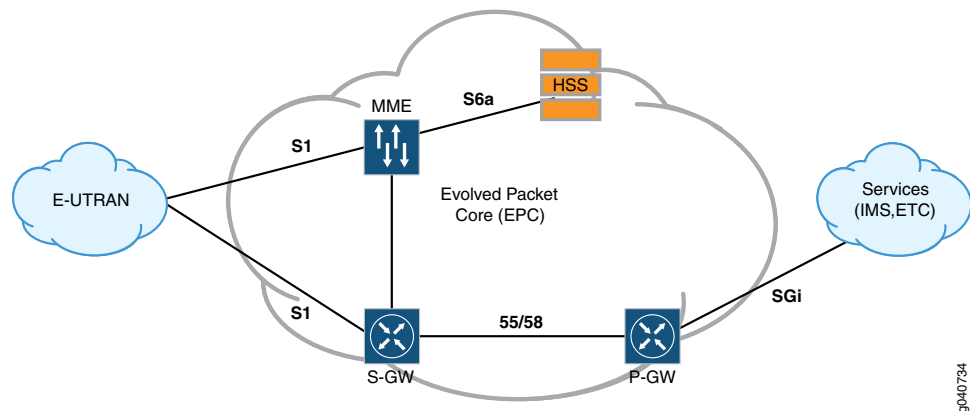
- [Overview of Mobile Networks on page 21](#)
- [Overview of APNs on page 28](#)
- [Overview of PDP Contexts and Bearers on page 30](#)
- [Overview of IPv6 and the Broadband Gateway on page 34](#)

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 8 on page 27](#) 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 8: 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**

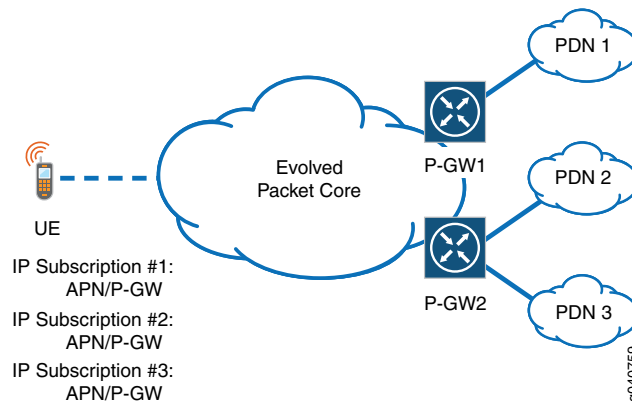
- [Overview of Mobile Networks on page 21](#)
- [Overview of Packet Data Network Gateway Functions on page 25](#)
- [Overview of APNs on page 28](#)
- [Overview of PDP Contexts and Bearers on page 30](#)
- [Overview of IPv6 and the Broadband Gateway on page 34](#)

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 9 on page 29](#) shows the relationship among APNs, P-GWs, and packet networks.

Figure 9: 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

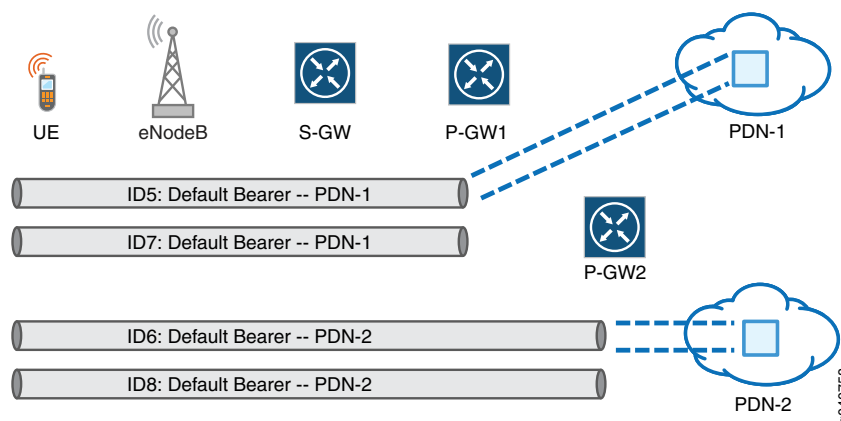
- [Overview of Mobile Networks on page 21](#)
- [Overview of Packet Data Network Gateway Functions on page 25](#)
- [Overview of PDP Contexts and Bearers on page 30](#)
- [Overview of IPv6 and the Broadband Gateway on page 34](#)

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 10 on page 30](#) shows the relationship between bearers and P-GWs.

Figure 10: 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

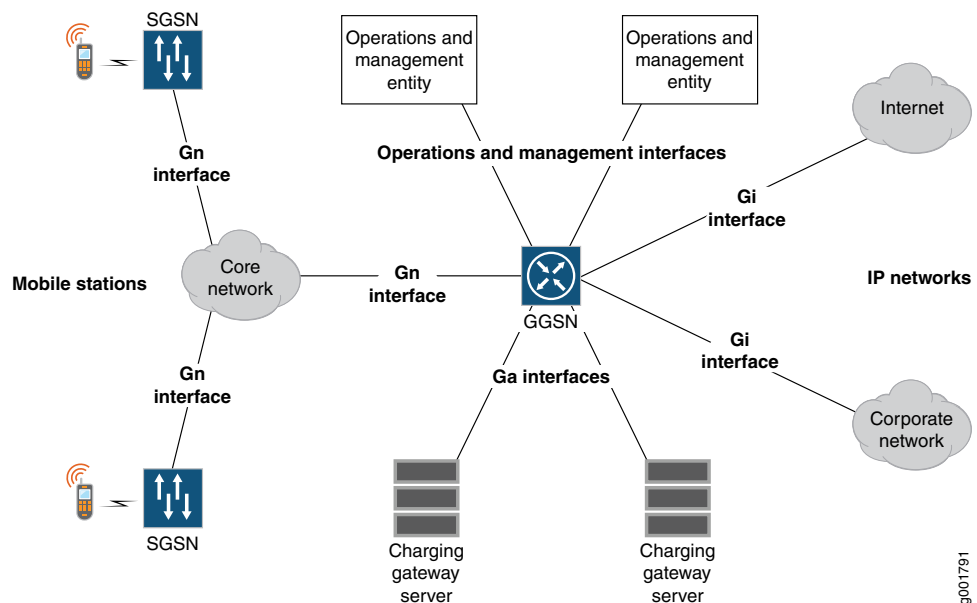
- [Overview of Mobile Networks on page 21](#)
- [Overview of Packet Data Network Gateway Functions on page 25](#)
- [Overview of APNs on page 28](#)
- [Overview of IPv6 and the Broadband Gateway on page 34](#)

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 11 on page 31](#) 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 11: 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**

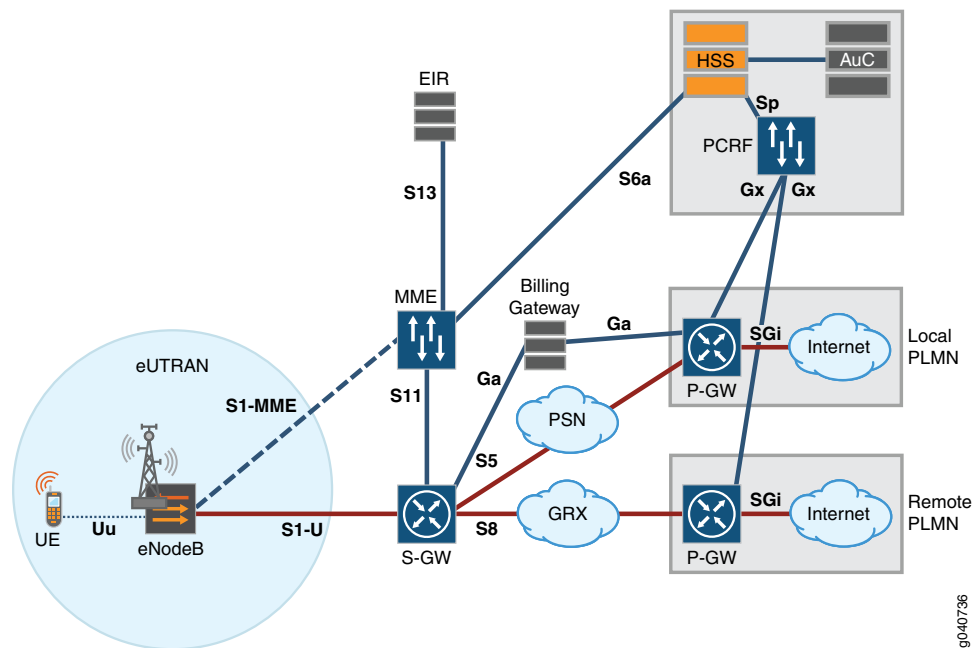
- [Overview of Mobile Networks on page 21](#)
- [Overview of Packet Data Network Gateway Functions on page 25](#)
- [Overview of APNs on page 28](#)
- [Overview of PDP Contexts and Bearers on page 30](#)
- [Overview of IPv6 and the Broadband Gateway on page 34](#)

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 12 on page 33](#) 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 12: 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 21](#)
- [Overview of Packet Data Network Gateway Functions on page 25](#)
- [Overview of APNs on page 28](#)
- [Overview of PDP Contexts and Bearers on page 30](#)
- [Overview of IPv6 and the Broadband Gateway on page 34](#)

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 21](#)
- [Overview of Packet Data Network Gateway Functions on page 25](#)
- [Overview of APNs on page 28](#)
- [Overview of PDP Contexts and Bearers on page 30](#)

PART 2

System Configuration

- [Configuring Mobility on MX 3D Devices on page 37](#)
- [Configuring Redundancy on MX 3D Devices on page 49](#)
- [Configuring Mobile Edge Exception Handling on page 63](#)

CHAPTER 3

Configuring Mobility on MX 3D Devices

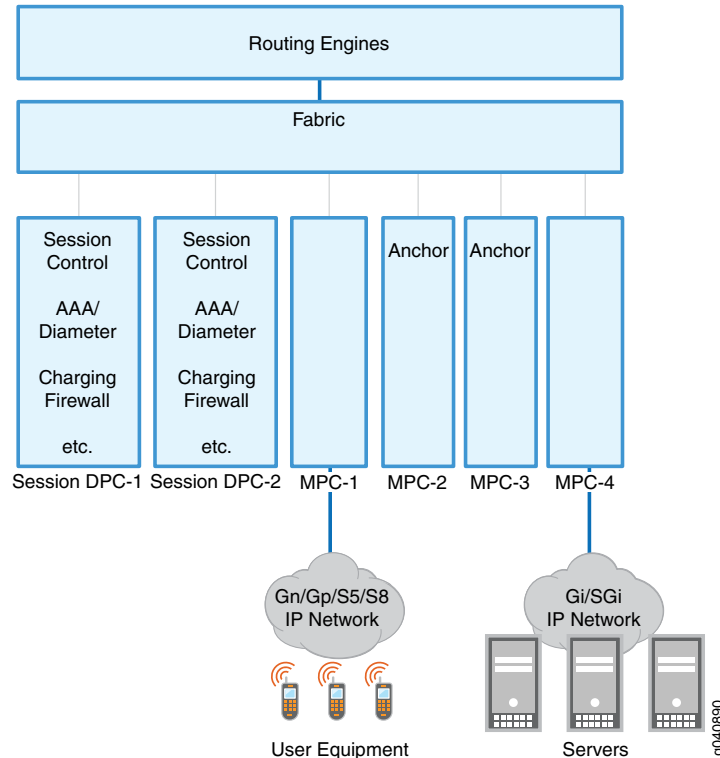
- [MobileNext Broadband Gateway Chassis Overview on page 38](#)
- [Configuring Session DPCs for Mobility on page 40](#)
- [Configuring Interface DPCs or MPCs for User Mobility Traffic on page 42](#)
- [Example: Configuring the MobileNext Broadband Gateway Chassis on page 43](#)
- [Understanding the MobileNext Broadband Gateway Anchors on page 45](#)
- [Configuring Anchor Session DPCs and PFEs on page 47](#)
- [Verifying the MobileNext Broadband Gateway Chassis Configuration on page 48](#)

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 13 on page 38](#), the session DPCs are shown on the left and the interface boards are shown as MPCs on the right.

Figure 13: Session DPCs and Interfaces on the Broadband Gateway



This chassis configuration overview covers:

- [Session DPCs for Mobility on page 39](#)
- [Overview of Mobility Interface Types on page 39](#)

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 43](#)
- [Configuring Session DPCs for Mobility on page 40](#)
- [Configuring Interface DPCs or MPCs for User Mobility Traffic on page 42](#)
- [Understanding the MobileNext Broadband Gateway Anchors on page 45](#)
- [Configuring Anchor Session DPCs and PFEs on page 47](#)
- [Verifying the MobileNext Broadband Gateway Chassis Configuration on page 48](#)

- [Overview of Broadband Gateway System Architecture on page 3](#)

Configuring Session DPCs for Mobility

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

Before you begin, you should have done the following:

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

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

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

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



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

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

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

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

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

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



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

Related Documentation

- [MobileNext Broadband Gateway Chassis Overview on page 38](#)
- [Example: Configuring the MobileNext Broadband Gateway Chassis on page 43](#)
- [Configuring Interface DPCs or MPCs for User Mobility Traffic on page 42](#)
- [Understanding the MobileNext Broadband Gateway Anchors on page 45](#)
- [Configuring Anchor Session DPCs and PFEs on page 47](#)
- [Verifying the MobileNext Broadband Gateway Chassis Configuration on page 48](#)
- [Overview of Broadband Gateway System Architecture on page 3](#)

Configuring Interface DPCs or MPCs for User Mobility Traffic

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

Before you begin, you should have done the following:

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

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

1. Configure the forwarding package at the FPC level (so that all Packet Forwarding Engines understand what to do with mobility packets) by configuring the **mobility ggsn-pgw** forwarding package at the FPC level.

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

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** forwarding package at the PIC level:

```
[edit chassis]
```

```
user@host# set fpc 0 pfe 0 forwarding-packages mobility ggsn-pgw
```

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 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 40](#)
- [Configuring Anchor Session DPCs and PFEs on page 47](#)
- [Verifying the MobileNext Broadband Gateway Chassis Configuration on page 48](#)

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 40](#)
- [Configuring Interface DPCs or MPCs for User Mobility Traffic on page 42](#)
- [Configuring Anchor Session DPCs and PFEs on page 47](#)
- [Verifying the MobileNext Broadband Gateway Chassis Configuration on page 48](#)

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 14: Upstream GTP-U Traffic

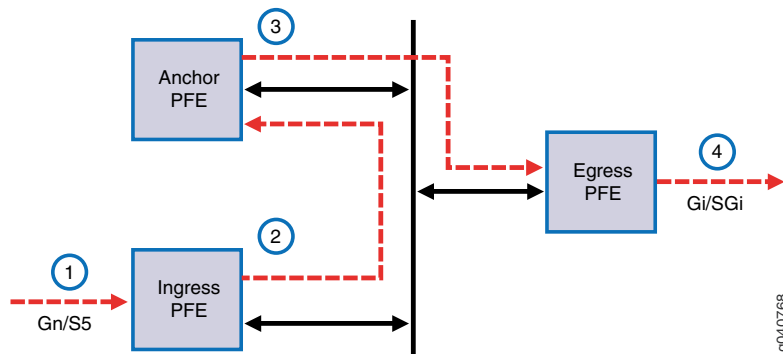


Figure 14 on page 46 shows how all GPRS tunneling protocol, user plane (GTP-U) traffic traverses an anchor Packet Forwarding Engine upstream from a Gn or S5 interface to a Gi or SGi interface:

- 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 15: Downstream GTP-U Traffic

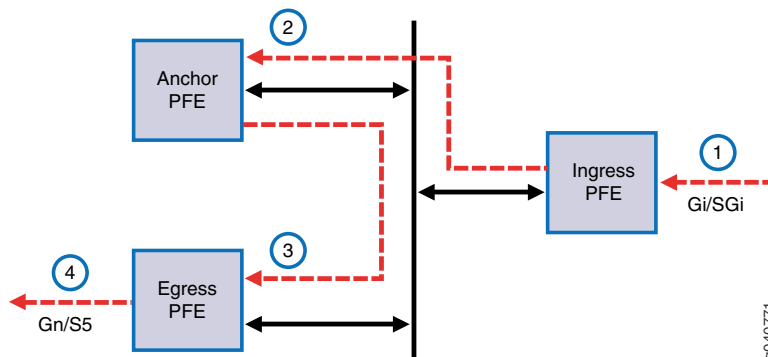


Figure 14 on page 46 shows how all GTP-U traffic traverses an anchor Packet Forwarding Engine downstream from a Gi or SGi interface to a Gn or S5 interface:

- 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 47](#)
- [MobileNext Broadband Gateway Chassis Overview on page 38](#)
- [Configuring Session DPCs for Mobility on page 40](#)
- [Configuring Interface DPCs or MPCs for User Mobility Traffic on page 42](#)
- [Verifying the MobileNext Broadband Gateway Chassis Configuration on page 48](#)

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 40](#)
- [Configuring Interface DPCs or MPCs for User Mobility Traffic on page 42](#)
- [Example: Configuring the MobileNext Broadband Gateway Chassis on page 43](#)
- [Verifying the MobileNext Broadband Gateway Chassis Configuration on page 48](#)

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 40](#)
- [Configuring Interface DPCs or MPCs for User Mobility Traffic on page 42](#)
- [Example: Configuring the MobileNext Broadband Gateway Chassis on page 43](#)
- [Configuring Anchor Session DPCs and PFEs on page 47](#)

CHAPTER 4

Configuring Redundancy on MX 3D Devices

- [Broadband Gateway Redundancy Overview on page 50](#)
- [Configuring Session DPC Redundancy on page 52](#)
- [Configuring Interface Redundancy on page 54](#)
- [Understanding the Broadband Gateway Anchor Failover Behavior on page 56](#)
- [Example: Configuring Broadband Gateway Redundancy on page 58](#)

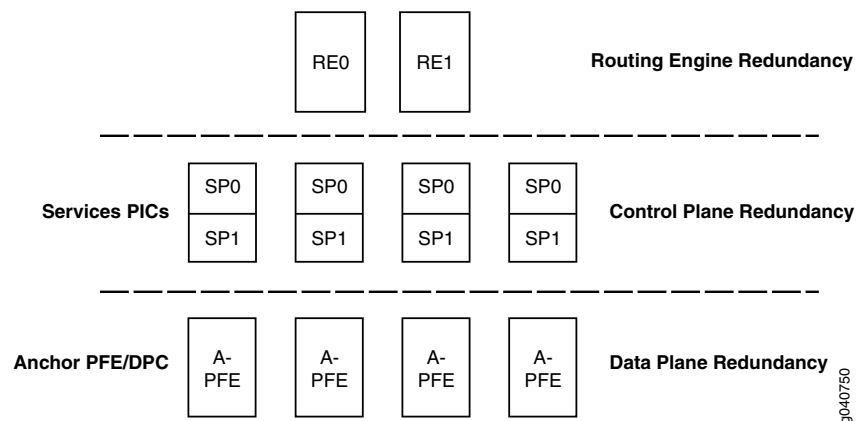
Broadband Gateway Redundancy Overview

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 16 on page 50 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 16: Redundancy Available on the Broadband Gateway



This redundancy configuration overview covers:

- [Routing Engine Redundancy on page 50](#)
- [Session DPC Redundancy on page 51](#)
- [Interface Redundancy on page 52](#)

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 52](#)
- [Configuring Interface Redundancy on page 54](#)
- [Understanding the Broadband Gateway Anchor Failover Behavior on page 56](#)
- [Example: Configuring Broadband Gateway Redundancy on page 58](#)
- [Configuring Anchor Session DPCs and PFEs on page 47](#)

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 50](#)
- [Configuring Interface Redundancy on page 54](#)
- [Understanding the Broadband Gateway Anchor Failover Behavior on page 56](#)
- [Example: Configuring Broadband Gateway Redundancy on page 58](#)
- [Configuring Anchor Session DPCs and PFEs on page 47](#)

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

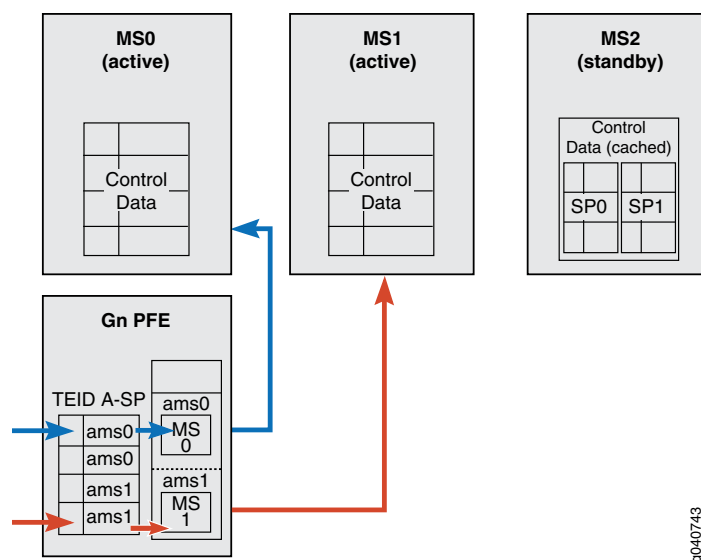
- [Broadband Gateway Redundancy Overview on page 50](#)
- [Configuring Session DPC Redundancy on page 52](#)
- [Understanding the Broadband Gateway Anchor Failover Behavior on page 56](#)

- [Example: Configuring Broadband Gateway Redundancy on page 58](#)
- [Configuring Anchor Session DPCs and PFEs on page 47](#)

Understanding the Broadband Gateway Anchor Failover Behavior

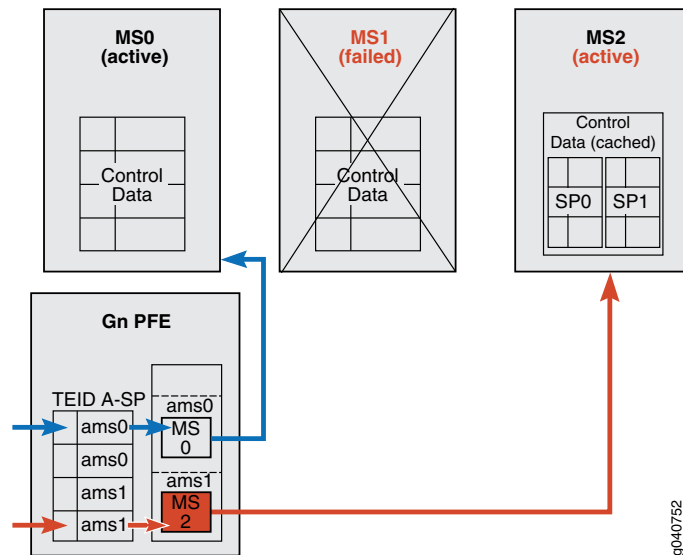
The MobileNext Broadband Gateway anchor session Dense Port Concentrators (DPCs) (housing PICs) and interface PFEs can be configured for redundancy. However, due to the different nature of the redundancy involved, 1:1 for anchor session PICs and N:1 for anchor interface PFEs, the failover behavior is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

Figure 17: Control Plane Anchor Operation Before Failure



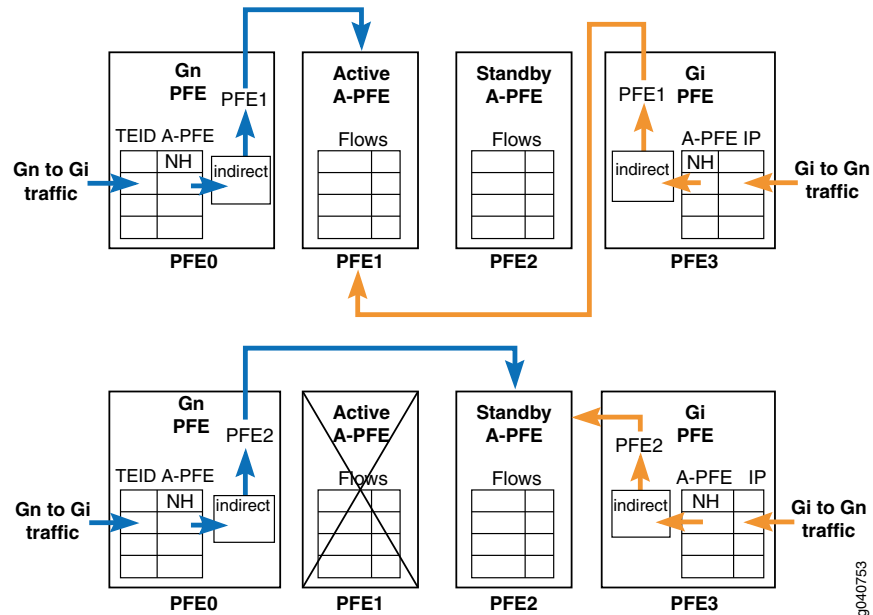
As shown in [Figure 17 on page 56](#), you can configure session DPCs with or without backup. In this case, **MS0** has no backup redundancy, while both PICs (PIC0 and PIC1) on **MS1** are backed up 1:1 by standby **MS2**. When the anchor session DPC **MS1** fails, packets cannot be processed strictly by hardware data path until the transfer of control to the new anchor is complete. This is shown in [Figure 18 on page 57](#). Note that **ams1** now points to **MS2**, the new active anchor.

Figure 18: 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 19 on page 57](#). For clarity, only the active and standby Packet Forwarding Engines are shown.

Figure 19: 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 50](#)
 - [Configuring Session DPC Redundancy on page 52](#)
 - [Configuring Interface Redundancy on page 54](#)
 - [Example: Configuring Broadband Gateway Redundancy on page 58](#)
 - [Configuring Anchor Session DPCs and PFEs on page 47](#)

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 58](#)
- [Overview on page 58](#)
- [Configuration on page 59](#)
- [Verification on page 61](#)

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

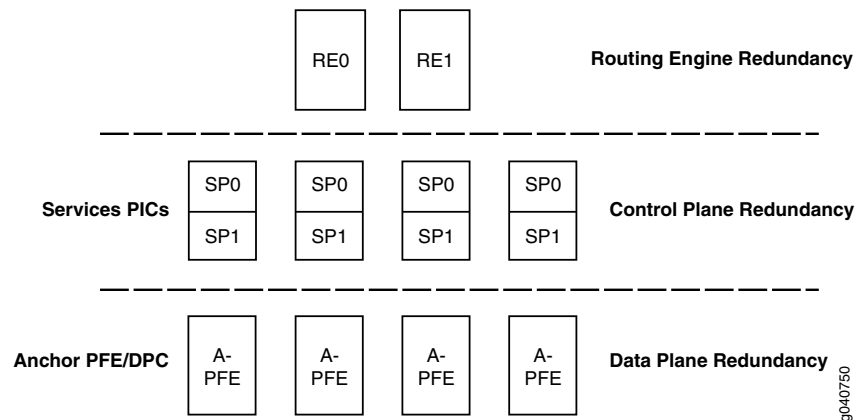
Before you begin:

- Install the chassis hardware.
- Configure the chassis.

Overview

[Figure 20 on page 59](#) 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 20: 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 59](#)

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 secundary 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 50](#)
 - [Configuring Session DPC Redundancy on page 52](#)
 - [Configuring Interface Redundancy on page 54](#)
 - [Understanding the Broadband Gateway Anchor Failover Behavior on page 56](#)
 - [Configuring Anchor Session DPCs and PFEs on page 47](#)

CHAPTER 5

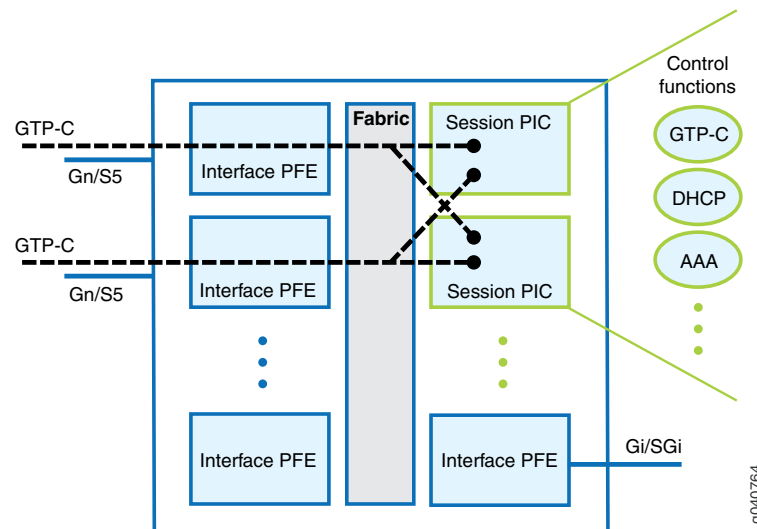
Configuring Mobile Edge Exception Handling

- [Understanding the Broadband Gateway Exception Handling on page 64](#)
- [Understanding GTP-U Error Exception Handling on page 65](#)
- [Understanding Broadband Gateway IP Fragment Handling on page 66](#)
- [Configuring Fragment Reassembly Parameters on page 66](#)
- [Understanding IPv6 Protocol Parameters on page 67](#)
- [Configuring IPv6 Protocol Parameters on page 68](#)
- [Configuring Exception Handling Traceoptions on page 70](#)
- [Example: Configuring Broadband Gateway Exception Handling Parameters on page 72](#)

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 21: GTP-C Handling



As shown in [Figure 21 on page 64](#), 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 65](#)
- [Understanding Broadband Gateway IP Fragment Handling on page 66](#)
- [Configuring Fragment Reassembly Parameters on page 66](#)
- [Understanding IPv6 Protocol Parameters on page 67](#)
- [Configuring IPv6 Protocol Parameters on page 68](#)
- [Configuring Exception Handling Traceoptions on page 70](#)
- [Example: Configuring Broadband Gateway Exception Handling Parameters on page 72](#)

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 64](#)
- [Understanding Broadband Gateway IP Fragment Handling on page 66](#)
- [Configuring Fragment Reassembly Parameters on page 66](#)
- [Understanding IPv6 Protocol Parameters on page 67](#)
- [Configuring IPv6 Protocol Parameters on page 68](#)
- [Configuring Exception Handling Traceoptions on page 70](#)
- [Example: Configuring Broadband Gateway Exception Handling Parameters on page 72](#)

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 64](#)
- [Understanding GTP-U Error Exception Handling on page 65](#)
- [Configuring Fragment Reassembly Parameters on page 66](#)
- [Understanding IPv6 Protocol Parameters on page 67](#)
- [Configuring IPv6 Protocol Parameters on page 68](#)
- [Configuring Exception Handling Traceoptions on page 70](#)
- [Example: Configuring Broadband Gateway Exception Handling Parameters on page 72](#)

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

reassemble 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 reassemble-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 reassemble-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 reassemble-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 64](#)
- [Understanding GTP-U Error Exception Handling on page 65](#)
- [Understanding Broadband Gateway IP Fragment Handling on page 66](#)
- [Understanding IPv6 Protocol Parameters on page 67](#)
- [Configuring IPv6 Protocol Parameters on page 68](#)
- [Configuring Exception Handling Traceoptions on page 70](#)
- [Example: Configuring Broadband Gateway Exception Handling Parameters on page 72](#)

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 64](#)
- [Understanding GTP-U Error Exception Handling on page 65](#)
- [Understanding Broadband Gateway IP Fragment Handling on page 66](#)
- [Configuring Fragment Reassembly Parameters on page 66](#)
- [Configuring IPv6 Protocol Parameters on page 68](#)
- [Configuring Exception Handling Traceoptions on page 70](#)
- [Example: Configuring Broadband Gateway Exception Handling Parameters on page 72](#)

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 64](#)
- [Understanding GTP-U Error Exception Handling on page 65](#)
- [Understanding Broadband Gateway IP Fragment Handling on page 66](#)
- [Configuring Fragment Reassembly Parameters on page 66](#)
- [Understanding IPv6 Protocol Parameters on page 67](#)
- [Configuring Exception Handling Traceoptions on page 70](#)
- [Example: Configuring Broadband Gateway Exception Handling Parameters on page 72](#)

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 10 on page 70](#) 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 10: Trace Flags

| Flag | Description |
|-------------|------------------|
| ager | Trace flow ager. |

Table 10: Trace Flags (*continued*)

| | |
|----------------------------------|--|
| 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 11 on page 71](#) describes the levels you can include.

Table 11: 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 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 64](#)
- [Understanding GTP-U Error Exception Handling on page 65](#)
- [Understanding Broadband Gateway IP Fragment Handling on page 66](#)
- [Configuring Fragment Reassembly Parameters on page 66](#)
- [Understanding IPv6 Protocol Parameters on page 67](#)
- [Configuring IPv6 Protocol Parameters on page 68](#)
- [Example: Configuring Broadband Gateway Exception Handling Parameters on page 72](#)

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 73](#)
- [Overview on page 73](#)
- [Configuration on page 73](#)
- [Verification on page 74](#)

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:

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

- [Understanding the Broadband Gateway Exception Handling on page 64](#)
- [Understanding GTP-U Error Exception Handling on page 65](#)
- [Understanding Broadband Gateway IP Fragment Handling on page 66](#)
- [Configuring Fragment Reassembly Parameters on page 66](#)
- [Understanding IPv6 Protocol Parameters on page 67](#)
- [Configuring IPv6 Protocol Parameters on page 68](#)
- [Configuring Exception Handling Traceoptions on page 70](#)

PART 3

APN Configuration

- [Configuring APNs on page 79](#)

CHAPTER 6

Configuring APNs

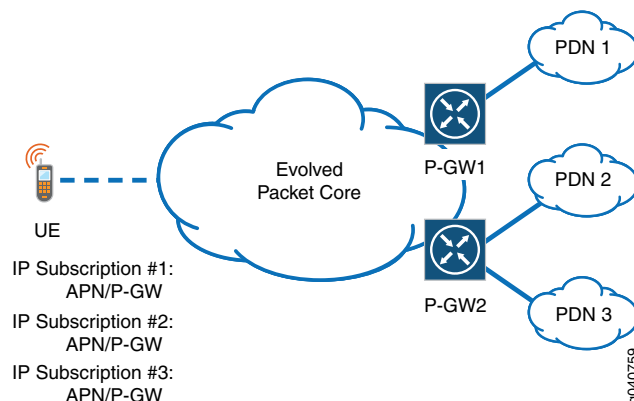
- [Configuring APNs on the MobileNext Broadband Gateway Overview on page 79](#)
- [User-Session Routing Overview on page 81](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 83](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 87](#)
- [Configuring Anonymous Users on a Broadband Gateway APN on page 88](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 89](#)
- [Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 93](#)
- [Configuring Mobile Interfaces for APNs on page 94](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 96](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 97](#)
- [Example: Configuring Broadband Gateway APNs on page 100](#)

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 22 on page 80](#) shows the relationship between APNs and broadband gateways in a 4G network.

Figure 22: 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 83](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 87](#)
- [Configuring Anonymous Users on a Broadband Gateway APN on page 88](#)
- [Configuring Anonymous Users on a Broadband Gateway APN on page 88](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 89](#)
- [Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 93](#)
- [Configuring Mobile Interfaces for APNs on page 94](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 96](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 97](#)
- [Example: Configuring Broadband Gateway APNs on page 100](#)

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 97](#)
- [Configuring APNs on the MobileNext Broadband Gateway Overview on page 79](#)

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 83](#)
- [Configuring Servers for an APN on page 84](#)
- [Configuring APN Timers on page 85](#)
- [Configuring Miscellaneous APN Parameters on page 85](#)

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 79](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 87](#)
- [Configuring Anonymous Users on a Broadband Gateway APN on page 88](#)
- [Configuring Anonymous Users on a Broadband Gateway APN on page 88](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 89](#)
- [Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 93](#)
- [Configuring Mobile Interfaces for APNs on page 94](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 96](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 97](#)
- [Example: Configuring Broadband Gateway APNs on page 100](#)

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 12 on page 88](#) 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 12: 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 79](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 83](#)
- [Configuring Anonymous Users on a Broadband Gateway APN on page 88](#)
- [Configuring Anonymous Users on a Broadband Gateway APN on page 88](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 89](#)
- [Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 93](#)
- [Configuring Mobile Interfaces for APNs on page 94](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 96](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 97](#)
- [Example: Configuring Broadband Gateway APNs on page 100](#)

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-msidn`, `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 79](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 83](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 87](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 89](#)
- [Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 93](#)
- [Configuring Mobile Interfaces for APNs on page 94](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 96](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 97](#)
- [Example: Configuring Broadband Gateway APNs on page 100](#)

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-instancerouting-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 79](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 83](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 87](#)

- [Configuring Anonymous Users on a Broadband Gateway APN on page 88](#)
- [Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 93](#)
- [Configuring Mobile Interfaces for APNs on page 94](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 96](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 97](#)
- [Example: Configuring Broadband Gateway APNs on page 100](#)

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 79](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 83](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 87](#)
- [Configuring Anonymous Users on a Broadband Gateway APN on page 88](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 89](#)
- [Configuring Mobile Interfaces for APNs on page 94](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 96](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 97](#)
- [Example: Configuring Broadband Gateway APNs on page 100](#)

Configuring Mobile Interfaces for APNs

You configure the MobileNext Broadband Gateway with mobile interfaces (**mif-**) for access point name (APN) traffic. The mobile interfaces are distinct from other type of interfaces and are used to associate an APN with a physical interface in a virtual routing and forwarding table (VRF). You need to configure one mobile interface unit for every APN. Every APN is associated with a single logical interface (unit) on a physical port represented by a mobile interface unit.

Before you begin, you should have done the following:

- Installed the broadband gateway

- Installed the boards of the broadband gateway
- Decided how many initial or additional APNs are required (you can add APNs after initial configuration)

To configure a mobile interface for mobility, you configure one or more logical interfaces (units) for the interface:

1. Configure the logical interface.

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

2. Optionally, configure the maximum transmission unit (MTU) size for the mobile interface.

```
[edit interfaces]
user@host# set mif mtu 1200
```



NOTE: MTU sizes are not mobility specific. However, MTU size is important because the GPRS tunneling protocol (GTP) header can cause a data unit to exceed the maximum frame size when the tunnel headers are added. This causes an error.

3. Optionally, configure the access control list (ACL) filters to apply to uplink and downlink traffic. By default, the APN accepts all mobile traffic. You can selectively accept or reject mobile traffic based on filter actions.

```
[edit interfaces]
user@host# set mif unit 0 filter input input-mif-unit0-filter
user@host# set mif unit 0 filter output output-mif-unit0-filter
```



NOTE: Filter configuration is not covered as part of mobility topics. The filtering is not mobility specific.

4. Optionally, configure the service filters to apply to uplink and downlink traffic at the APN level. Typically, these filters would provide services such as Network Address translation (NAT) to mobile traffic. By default, no such services are applied to mobile traffic:

```
[edit interfaces]
user@host# set mif unit 0 service input service-filter input-service-unit0 service-set
nat-service-unit0
user@host# set mif unit 0 service output service-filter input-service-unit0 service-set
nat-service-unit0
```



NOTE: Service filter configuration is not covered as part of mobility topics. Service filtering is not mobility specific.

Related Documentation

- [Configuring APNs on the MobileNext Broadband Gateway Overview on page 79](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 83](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 87](#)
- [Configuring Anonymous Users on a Broadband Gateway APN on page 88](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 89](#)
- [Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 93](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 96](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 97](#)
- [Example: Configuring Broadband Gateway APNs on page 100](#)

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 79](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 83](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 87](#)
- [Configuring Anonymous Users on a Broadband Gateway APN on page 88](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 89](#)
- [Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 93](#)
- [Configuring Mobile Interfaces for APNs on page 94](#)
- [Configuring APN Service Selection on a Broadband Gateway on page 97](#)
- [Example: Configuring Broadband Gateway APNs on page 100](#)

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 79](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 83](#)
- [Configuring the Restriction Value on a Broadband Gateway APN on page 87](#)
- [Configuring Anonymous Users on a Broadband Gateway APN on page 88](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 89](#)
- [Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 93](#)
- [Configuring Mobile Interfaces for APNs on page 94](#)
- [Configuring Mobile Interface to APN Associations in VRFs on page 96](#)
- [Example: Configuring Broadband Gateway APNs on page 100](#)

Example: Configuring Broadband Gateway APNs

This example shows how to configure an access point network (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 100](#)
- [Overview on page 100](#)
- [Configuration on page 101](#)
- [Verification on page 103](#)

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

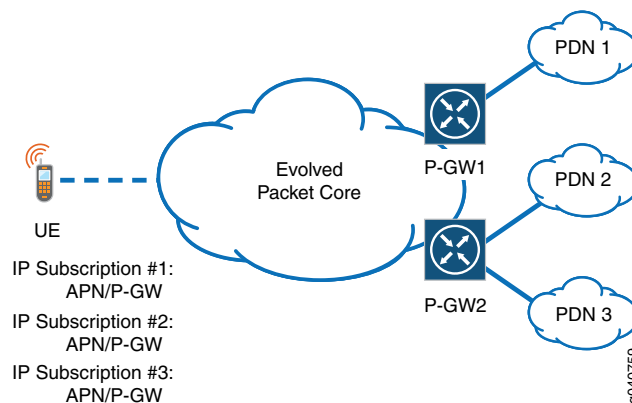
Before you begin:

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

Overview

[Figure 23 on page 101](#) 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 23: 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 79 • Configuring General APN Parameters on the Broadband Gateway on page 83 • Configuring the Restriction Value on a Broadband Gateway APN on page 87 • Configuring Anonymous Users on a Broadband Gateway APN on page 88 • Configuring Address Assignment on a Broadband Gateway APN on page 89 • Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 93 • Configuring Mobile Interfaces for APNs on page 94 • Configuring Mobile Interface to APN Associations in VRFs on page 96 |

- [Configuring APN Service Selection on a Broadband Gateway on page 97](#)

PART 4

Authorization and Addressing Configuration

- [Configuring AAA on page 107](#)
- [Configuring DHCP on page 167](#)

CHAPTER 7

Configuring AAA

- Overview of AAA on the Broadband Gateway on page 108
- Scalability and Redundancy on page 110
- Network Elements on page 111
- Network Element Groups on page 112
- AAA Profiles on page 113
- Supported Attributes in Access-Request Messages on page 115
- Supported Attributes in Access-Accept Messages on page 119
- Supported Attributes in Accounting Start Messages on page 122
- Supported Attributes in Accounting Interim Update Messages on page 126
- Supported Attributes in Accounting Stop Messages on page 131
- Supported Attributes in Accounting On Messages on page 135
- Supported Attributes in Disconnect Request Messages on page 136
- Supported Attributes in Change of Authorization (CoA) Messages on page 137
- Configuring AAA on the Broadband Gateway on page 139
- Configuring Interaction Between the Broadband Gateway and RADIUS Servers on page 139
- Configuring RADIUS-Initiated Dynamic Request Support on page 141
- Configuring Dead Server Detection on page 141
- Configuring Network Elements on page 142
- Configuring Network Element Groups on page 143
- Configuring an AAA Profile on page 144
- Configuring Authentication Settings in an AAA Profile on page 144
- Configuring Accounting Settings in an AAA Profile on page 145
- Configuring RADIUS Attribute Usage for an AAA Profile on page 146
- Specifying RADIUS Options in an AAA Profile on page 150
- Applying an AAA Profile to an APN on page 150
- Enabling Address Assignment by the RADIUS Server on page 151

- [Configuring AAA-Assigned Addresses to Override Locally or DHCP-Assigned Addresses on page 151](#)
- [Configuring the Broadband Gateway to Wait for an Accounting Response on page 152](#)
- [Example: Configuring AAA on the Broadband Gateway on page 152](#)

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 137](#) 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 136](#) 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 115](#) and [“Supported Attributes in Access-Accept Messages” on page 119](#) describe how the broadband gateway processes these attributes and VSAs.

Related Documentation

- [Configuring APNs on the MobileNext Broadband Gateway Overview on page 79](#)
- [Configuring AAA on the Broadband Gateway on page 139](#)
- [Configuring Anonymous Users on a Broadband Gateway APN on page 88](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 89](#)
- [Example: Configuring AAA on the Broadband Gateway on page 152](#)

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 38](#)
- [Broadband Gateway Redundancy Overview on page 50](#)
- [Network Elements on page 111](#)
- [Network Element Groups on page 112](#)

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 113](#)
- [Configuring Network Elements on page 142](#)
- [Network Element Groups on page 112](#)

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 113](#)
- [Configuring Network Elements on page 142](#)
- [Configuring Network Element Groups on page 143](#)

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 144](#)
- [Configuring Network Elements on page 142](#)
- [Configuring Network Element Groups on page 143](#)

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 115](#)
- [3GPP VSAs Supported in Access-Request Messages on page 117](#)

RADIUS IETF Attributes Supported in Access-Request Messages

Table 13 on page 115 lists the RADIUS attributes supported by the broadband gateway in Access-Request messages.

Table 13: 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 13: 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 | The CHAP Challenge is provided to the broadband gateway by the user in the PCO received during the IP-CAN session establishment procedure. If the PPP PDP type is used, it is provided to the broadband gateway by the user during the PPP authentication phase. | String |

Table 13: 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 14 on page 117 lists the 3GPP vendor-specific attributes (VSAs) supported by the broadband gateway in Access-Request messages.

Table 14: 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 14: 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 14: 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 120](#)
- [3GPP VSAs Supported in Access-Accept Messages on page 121](#)
- [Juniper Networks VSAs Supported in Access-Accept Messages on page 122](#)

RADIUS IETF Attributes Supported in Access-Accept Messages

Table 15 on page 120 lists the RADIUS attributes supported by the broadband gateway in Access-Accept messages.

Table 15: 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 15: 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 17 on page 122 lists the 3GPP vendor-specific attributes (VSAs) supported by the broadband gateway in Access-Accept messages.

Table 16: 3GPP VSAs Supported in Access-Accept Messages

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

Table 16: 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 17 on page 122](#) lists the Juniper Networks VSAs supported by the broadband gateway in Access-Accept messages.

Table 17: 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 122](#)
- [3GPP VSAs Supported in Accounting Start Messages on page 124](#)

RADIUS IETF Attributes Supported in Accounting Start Messages

[Table 18 on page 123](#) lists the RADIUS attributes supported by the broadband gateway in Accounting Start messages.

Table 18: 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 18: 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 19 on page 124 lists the 3GPP vendor-specific attributes (VSAs) supported by the broadband gateway in Accounting Start messages.

Table 19: 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-GPS-Negotiated-QoS-Profiles | QoS profile applied by the broadband gateway for the PDP context/EPS bearer | UTF-8 encoded string |

Table 19: 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 19: 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 126](#)
- [3GPP VSAs Supported in Interim-Update Messages on page 128](#)

RADIUS IETF Attributes Supported in Interim-Update Messages

[Table 20 on page 127](#) lists the RADIUS attributes supported by the broadband gateway in Interim-Update messages.

Table 20: 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 20: 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 21 on page 129 lists the 3GPP vendor-specific attributes (VSAs) supported by the broadband gateway in Interim-Update messages.

Table 21: 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 21: 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 131](#)
- [3GPP VSAs Supported in Accounting Stop Messages on page 133](#)

RADIUS IETF Attributes Supported in Accounting Stop Messages

[Table 22 on page 131](#) lists the RADIUS attributes supported by the broadband gateway in Accounting Stop messages.

Table 22: 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 22: 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 22: 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 23 on page 133 lists the 3GPP vendor-specific attributes (VSAs) supported by the broadband gateway in Accounting Stop messages.

Table 23: 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 23: 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 23: 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 135](#)

RADIUS IETF Attributes Supported in Accounting On Messages

[Table 24 on page 136](#) lists the RADIUS attributes supported by the broadband gateway in Accounting On messages.

Table 24: 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 136](#)
- [3GPP VSAs Supported in Disconnect Request Messages on page 137](#)

RADIUS IETF Attributes Supported in Disconnect Request Messages

[Table 25 on page 136](#) lists the RADIUS attributes supported by the broadband gateway in Disconnect Request messages.

Table 25: 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 25: 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 26 on page 137 lists the 3GPP VSAs supported by the broadband gateway in Disconnect Request messages.

Table 26: 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 137](#)
- [3GPP VSAs Supported in CoA Messages on page 138](#)

RADIUS IETF Attributes Supported in CoA Messages

Table 27 on page 138 lists the RADIUS attributes supported by the broadband gateway in CoA messages.

Table 27: 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 28 on page 138 lists the 3GPP vendor-specific attributes (VSAs) supported by the broadband gateway in CoA messages.

Table 28: 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 139.](#)
2. Configure one or more network elements.
See [“Configuring Network Elements” on page 142.](#)
3. (Optional) Configure a network element group to use with accounting.
See [“Configuring Network Element Groups” on page 143.](#)
4. Configure an AAA profile.
See [“Configuring an AAA Profile” on page 144.](#)
5. Configure AAA services for an APN.
See [“Applying an AAA Profile to an APN” on page 150.](#)



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 108](#)
- [Network Elements on page 111](#)
- [Network Element Groups on page 112](#)
- [AAA Profiles on page 113](#)
- [Mobility Maintenance Mode Overview on page 318](#)
- [Modifying an Access Point Name on page 322](#)

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 108](#)
- [Example: Configuring AAA on the Broadband Gateway on page 152](#)

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 108](#)
- [Example: Configuring AAA on the Broadband Gateway on page 152](#)

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 108](#)
- [Example: Configuring AAA on the Broadband Gateway on page 152](#)

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 111](#)
- [Network Element Groups on page 112](#)
- [Example: Configuring AAA on the Broadband Gateway on page 152](#)

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 112](#)
- [Network Elements on page 111](#)
- [Example: Configuring AAA on the Broadband Gateway on page 152](#)

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 144](#).

3. Configure accounting settings for the AAA profile.

See [“Configuring Accounting Settings in an AAA Profile” on page 145](#).

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 146](#).

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 150](#).

Related Documentation

- [Overview of AAA on the Broadband Gateway on page 108](#)
- [AAA Profiles on page 113](#)
- [Example: Configuring AAA on the Broadband Gateway on page 152](#)

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 113](#)
- [Network Elements on page 111](#)
- [Example: Configuring AAA on the Broadband Gateway on page 152](#)

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 29 on page 145](#) 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 29 on page 145](#) lists the events you can specify.

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

Table 29: 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 29: 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 108](#)
- [AAA Profiles on page 113](#)
- [Network Elements on page 111](#)
- [Network Element Groups on page 112](#)
- [Example: Configuring AAA on the Broadband Gateway on page 152](#)

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 30 on page 147](#) 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 31 on page 147](#) for the RADIUS attributes and message type combinations you can configure. See [Table 32 on page 148](#) 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 32 on page 148](#) 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 30 on page 147](#) lists the attributes supported in the **ignore** statement.

Table 30: 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 31 on page 147](#) lists the RADIUS attributes and message types supported in the **exclude** statement.

Table 31: 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 31: 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 32 on page 148](#) 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 32: 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 32: 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 108](#)
- [AAA Profiles on page 113](#)
- [Example: Configuring AAA on the Broadband Gateway on page 152](#)

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 113](#)
- [Example: Configuring AAA on the Broadband Gateway on page 152](#)

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 79](#)
 - [AAA Profiles on page 113](#)
 - [Example: Configuring AAA on the Broadband Gateway on page 152](#)

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 89](#)
 - [Example: Configuring AAA on the Broadband Gateway on page 152](#)

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 89](#)
 - [Example: Configuring AAA on the Broadband Gateway on page 152](#)

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 108](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 83](#)

Example: Configuring AAA on the Broadband Gateway

- [Requirements on page 152](#)
- [Overview on page 152](#)
- [Configuration on page 155](#)
- [Verification on page 163](#)

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 155](#)
- [Configuring the Loopback Interface on page 158](#)
- [Configuring the Network Elements on page 159](#)
- [Configuring the Network Element Group on page 160](#)
- [Configuring the AAA Profile on page 160](#)
- [Applying AAA Services to an APN on page 162](#)

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 108](#)
 - [Configuring AAA on the Broadband Gateway on page 139](#)
 - [Configuring APNs on the MobileNext Broadband Gateway Overview on page 79](#)
 - [Configuring Anonymous Users on a Broadband Gateway APN on page 88](#)
 - [Configuring Address Assignment on a Broadband Gateway APN on page 89](#)

CHAPTER 8

Configuring DHCP

- [DHCP Overview on page 167](#)
- [DHCP Proxy Client on page 168](#)
- [Configuring DHCP Proxy Client on page 168](#)
- [Configuring DHCP Under APN on page 169](#)

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 173](#)

CHAPTER 9

Configuring GTP

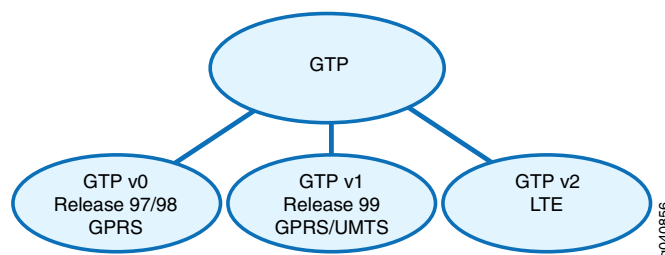
- [GTP Versions and GPRS Interfaces Overview on page 174](#)
- [GPRS Tunneling Protocol \(GTP\) Overview on page 175](#)
- [GTP Path Management Overview on page 176](#)
- [Understanding Path Management on page 177](#)
- [GTP Tunnel Management Overview on page 180](#)
- [Understanding Tunnel Management on page 181](#)
- [Restart Counters Overview on page 183](#)
- [Understanding CSID Signaling on page 184](#)
- [Understanding Tunnel Endpoint Identifiers on page 185](#)
- [Configuring GTP Services Overview on page 186](#)
- [Configuring a Loopback Interface for Transport of GTP Packets on page 188](#)
- [Configuring GTP Services on a Broadband Gateway on page 189](#)
- [Configuring GTP Services on the Control Plane on page 190](#)
- [Configuring GTP Services on the Data Plane on page 192](#)
- [Configuring GTP Services on the S5 Interface on page 193](#)
- [Configuring GTP Services on the S8 Interface on page 195](#)
- [Configuring GTP Services on the Gn Interface on page 196](#)
- [Configuring GTP Services on the Gp Interface on page 198](#)
- [Configuring GTP Services When the S5 and S8 Interfaces Are in Different VRFs on page 199](#)
- [Configuring GTP Services When the S5 and S8 Interfaces Are in the Same VRF on page 201](#)
- [Configuring GTP Services When 3GPP Interfaces Are in Different VRFs on page 202](#)
- [Configuring GTP Services on a GGSN Broadband Gateway on page 204](#)
- [Configuring GTP Services on a Peer Group on page 205](#)
- [Disabling Path Management on a Broadband Gateway or Peer Group on page 206](#)
- [Configuring GTP Trace Options on page 207](#)

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 24 on page 174 shows the GTP versions that the broadband gateway supports.

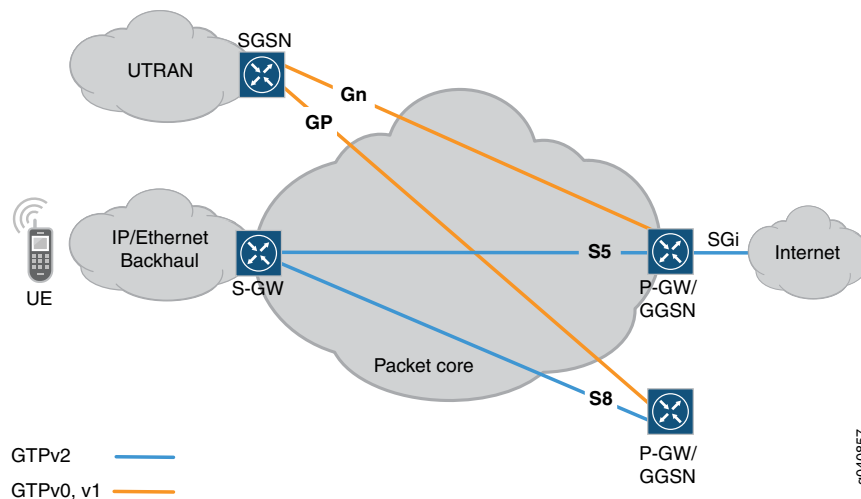
Figure 24: GTP Versions Supported on a MobileNext Broadband Gateway



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 25 on page 174 shows the GTP-C versions the broadband gateway supports for the 3G and 4G network interfaces.

Figure 25: 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 175](#)
- [GTP Tunnel Management Overview on page 180](#)

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 186](#)
- [GTP Path Management Overview on page 176](#)
- [GTP Tunnel Management Overview on page 180](#)

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 176](#)
- [GTP Version Support for Echo Requests and Echo Responses on page 177](#)

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 186](#)
- [GTP Tunnel Management Overview on page 180](#)
- [Understanding Tunnel Endpoint Identifiers on page 185](#)

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:

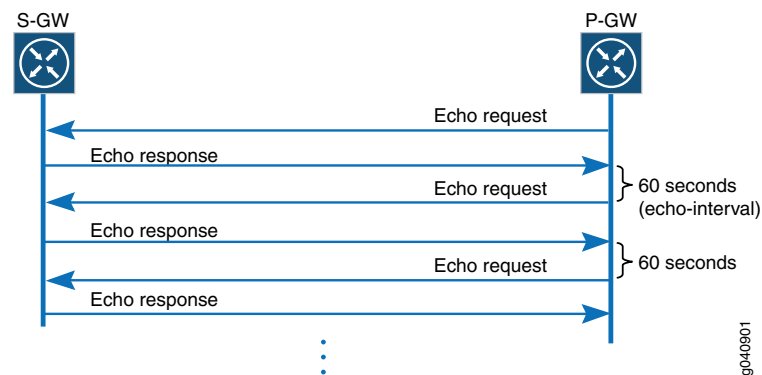
- [Successful Echo-Request Sequence for Path Management on page 177](#)
- [Failed Echo Request Sequence for Path Management on page 178](#)

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 26 on page 178](#) shows a successful echo-request sequence, in which the P-GW receives an echo response for each echo request.

Figure 26: Successful Echo-Request Sequence for Path Management



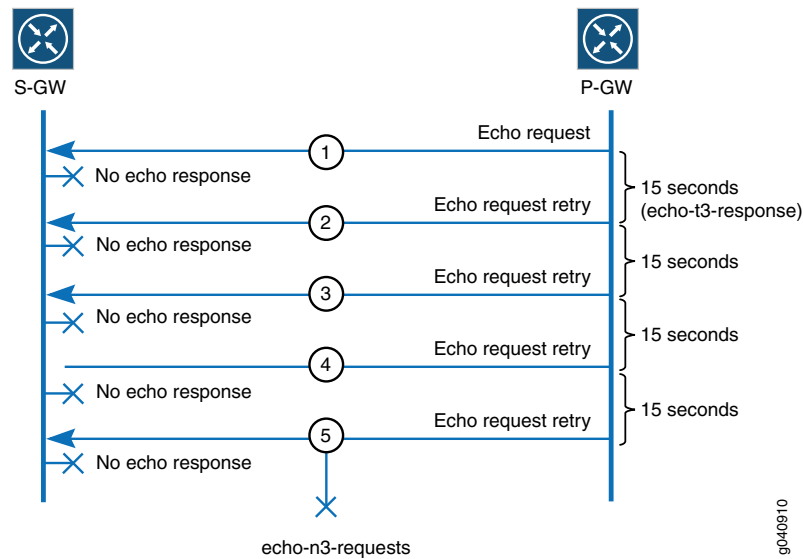
The following steps describe the echo request/response sequence in [Figure 26 on page 178](#):

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 27 on page 179](#) 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 27: Failed Echo-Request Sequence for Path Management



The following steps describe the echo-request and echo-response sequence in [Figure 27 on page 179](#):

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 186](#)
- [GTP Path Management Overview on page 176](#)
- [GTP Tunnel Management Overview on page 180](#)
- [Understanding Tunnel Endpoint Identifiers on page 185](#)

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 180](#)
- [Default Tunnel Management Configuration on page 180](#)
- [GTP Version Support for Tunnel Management Requests and Responses on page 180](#)

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 186](#)
- [GTP Path Management Overview on page 176](#)
- [Understanding Tunnel Endpoint Identifiers on page 185](#)

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.

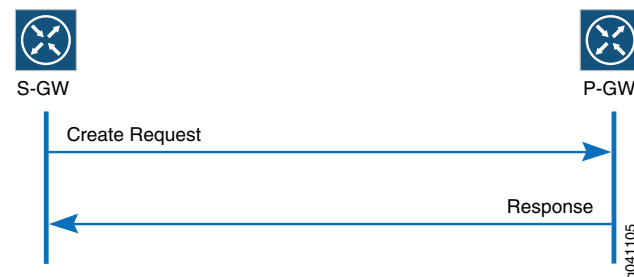
This topic covers:

- [Successful Create Request Sequence for Tunnel Management on page 181](#)
- [Successful Update/Delete Request Sequence for Tunnel Management on page 181](#)
- [Failed Update/Delete Request Sequence for Tunnel Management on page 182](#)

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 28 on page 181](#) shows a successful Create request sequence in which the S-GW receives a response after sending a request.

Figure 28: Successful Create Request Sequence for Tunnel Management



The following steps describe the tunnel management Create request sequence in [Figure 28 on page 181](#):

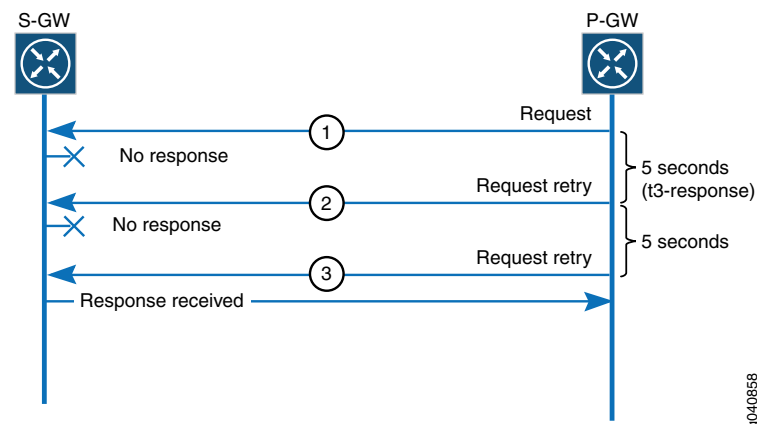
1. The S-GW sends a Create request message to the P-GW.
2. The P-GW sends a response back to the S-GW.

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 29 on page 182](#) 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 29: Successful Update/Delete Request Sequence for Tunnel Management



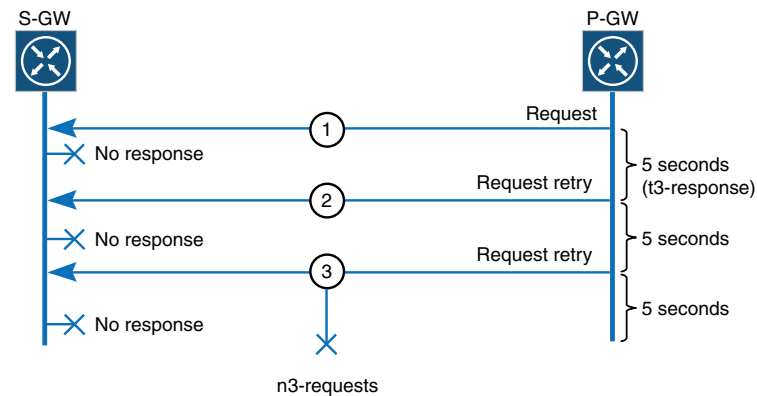
The following steps describe the tunnel management Update or Delete request sequence in [Figure 29 on page 182](#):

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 30 on page 183](#) 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 30: Failed Update/Delete Request Sequence for Tunnel Management



g040900

The following steps describe the Update or Delete request failed sequence in [Figure 30 on page 183](#):

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 186](#)
- [GTP Path Management Overview on page 176](#)
- [GTP Tunnel Management Overview on page 180](#)
- [Understanding Tunnel Endpoint Identifiers on page 185](#)

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 186](#)
- [GTP Path Management Overview on page 176](#)
- [GTP Tunnel Management Overview on page 180](#)

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**

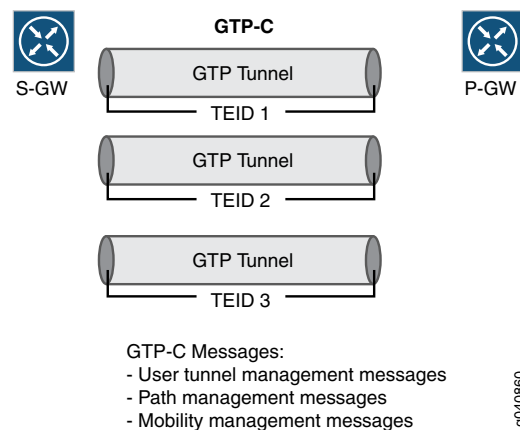
- [GPRS Tunneling Protocol \(GTP\) Overview on page 175](#)
- [GTP Path Management Overview on page 176](#)
- [GTP Tunnel Management Overview on page 180](#)
- [Understanding Tunnel Endpoint Identifiers on page 185](#)

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 31 on page 185 shows a GTP tunnel with its associated TEID.

Figure 31: 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 31 on page 185. 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 186](#)
- [GTP Path Management Overview on page 176](#)

- [GTP Tunnel Management Overview on page 180](#)

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 186](#)
- [Configuring GTP Services at Different Levels on a Broadband Gateway on page 186](#)
- [GTP Services Default Settings on page 187](#)
- [GTP Version Support on page 188](#)

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 176](#).

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 180](#).

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 175](#)
- [GTP Path Management Overview on page 176](#)
- [GTP Tunnel Management Overview on page 180](#)

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 189](#)

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 188](#)
- [Configuring GTP Services on the Data Plane on page 192](#)
[Configuring GTP Services on the Control Plane on page 190](#)
- [Configuring GTP Services Overview on page 186](#)

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 188](#)
- [Configuring GTP Services on the Data Plane on page 192](#)
- [Configuring GTP Services on a Broadband Gateway on page 189](#)
- [Configuring GTP Services Overview on page 186](#)

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 185](#)
 - [Configuring a Loopback Interface for Transport of GTP Packets on page 188](#)
 - [Configuring GTP Services on the Control Plane on page 190](#)
 - [Configuring GTP Services on a Broadband Gateway on page 189](#)
 - [Configuring GTP Services Overview on page 186](#)

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 188](#)
- [Configuring GTP Services on the S8 Interface on page 195](#)
- [Configuring GTP Services on the Data Plane on page 192](#)
- [Configuring GTP Services on the Control Plane on page 190](#)
- [Configuring GTP Services on a Broadband Gateway on page 189](#)
- [Configuring GTP Services Overview on page 186](#)

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 188](#)
- [Configuring GTP Services on the S5 Interface on page 193](#)
- [Configuring GTP Services on the Data Plane on page 192](#)
- [Configuring GTP Services on the Control Plane on page 190](#)
- [Configuring GTP Services on a Broadband Gateway on page 189](#)
- [Configuring GTP Services Overview on page 186](#)

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 188](#)
- [Configuring GTP Services on the Gp Interface on page 198](#)
- [Configuring GTP Services on the Data Plane on page 192](#)
- [Configuring GTP Services on the Control Plane on page 190](#)
- [Configuring GTP Services on a Broadband Gateway on page 189](#)
- [Configuring GTP Services Overview on page 186](#)

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 188](#)
- [Configuring GTP Services on the Gn Interface on page 196](#)
- [Configuring GTP Services on the Data Plane on page 192](#)
- [Configuring GTP Services on the Control Plane on page 190](#)
- [Configuring GTP Services on a Broadband Gateway on page 189](#)
- [Configuring GTP Services Overview on page 186](#)

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
```

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
```

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 188](#)
- [Configuring GTP Services on the Data Plane on page 192](#)
- [Configuring GTP Services on the Control Plane on page 190](#)
- [Configuring GTP Services on a Broadband Gateway on page 189](#)
- [Configuring GTP Services Overview on page 186](#)

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
```

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
```

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 188](#)
- [Configuring GTP Services on the Data Plane on page 192](#)
- [Configuring GTP Services on the Control Plane on page 190](#)
- [Configuring GTP Services on a Broadband Gateway on page 189](#)
- [Configuring GTP Services Overview on page 186](#)

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 188](#)
- [Configuring GTP Services on the Data Plane on page 192](#)
- [Configuring GTP Services on the Control Plane on page 190](#)

- [Configuring GTP Services on a Broadband Gateway on page 189](#)
- [Configuring GTP Services Overview on page 186](#)

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 188](#)
- [Configuring GTP Services Overview on page 186](#)
- [Configuring GTP Services on the Data Plane on page 192](#)
- [Configuring GTP Services on the Control Plane on page 190](#)
- [Configuring GTP Services on a Broadband Gateway on page 189](#)
- [Configuring GTP Services When 3GPP Interfaces Are in Different VRFs on page 202](#)

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 188](#)
- [Configuring GTP Services on the Data Plane on page 192](#)
- [Configuring GTP Services on the Control Plane on page 190](#)
- [Configuring GTP Services on a Broadband Gateway on page 189](#)
- [Configuring GTP Services Overview on page 186](#)

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 176](#)
 - [Configuring GTP Services Overview on page 186](#)

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 33 on page 207](#) describes the flags that you can include.

Table 33: Trace Flags

| Flag | Description |
|------------------|--|
| all | Trace everything. |
| config | Trace configuration-related information. |
| debug | Trace debug information. |
| 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 34 on page 207](#) describes the levels you can include.

Table 34: Trace Levels

| Level | Description |
|------------|-------------------|
| all | Match all levels. |

Table 34: Trace Levels (*continued*)

| | |
|----------------|--|
| 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 ggsn-pgw pgw-1 gtp]
user@host# edit traceoptions
```
2. 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
```
3. (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
```
4. 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 186](#)

PART 6

Charging Configuration

- [Charging Overview on page 211](#)
- [Configuring Charging on page 219](#)

CHAPTER 10

Charging Overview

- [Charging on page 211](#)
- [Charging Services Overview on page 211](#)
- [Charging Data Records on page 213](#)
- [Charging Profiles on page 217](#)

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 211](#)

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

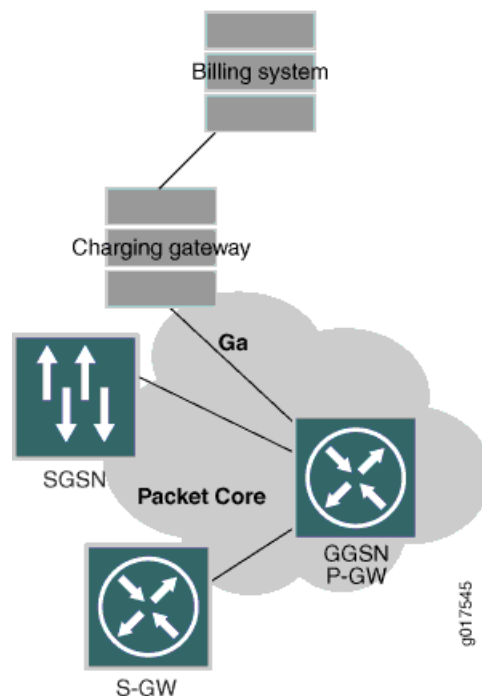
record collection for their mobile subscribers. The broadband gateway gathers Charging Data Records (CDRs) and delivers them to the charging gateway function (CGF) over the Ga interface using the GTP Prime protocol. The billing function is distributed across all modules of the broadband gateway, which 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 32 on page 212 shows the components in a sample charging topology.

Figure 32: 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 220](#)
- [Configuring Persistent Storage on page 222](#)
- [Charging Data Records on page 213](#)
- [Charging Profiles on page 217](#)

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 219](#)
- [Configuring Transport Profiles on page 226](#)

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 231](#)
- [Configuring Transport Profiles on page 226](#)
- [Configuring Charging Trigger Events on page 227](#)
- [Configuring CDR Attributes on page 229](#)
- [Configuring Charging Profiles for APNs on page 232](#)

Configuring Charging

- [Configuring Charging on page 219](#)
- [Configuring GTP Prime for Charging on page 220](#)
- [Configuring Persistent Storage on page 222](#)
- [Configuring the Solid State Disk for Persistent Storage on page 224](#)
- [Configuring Transport Profiles on page 226](#)
- [Configuring Charging Trigger Events on page 227](#)
- [Configuring CDR Attributes on page 229](#)
- [Configuring Charging Profiles on page 231](#)
- [Configuring Charging Profiles for APNs on page 232](#)
- [Tracing Charging Operations on page 233](#)
- [Verifying and Managing the Charging Configuration on page 235](#)

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 220](#)
- [Configuring Persistent Storage on page 222](#)
- [Configuring Transport Profiles on page 226](#)
- [Configuring Charging Trigger Events on page 227](#)
- [Configuring CDR Attributes on page 229](#)
- [Configuring Charging Profiles on page 231](#)
- [Configuring Charging Profiles for APNs on page 232](#)
- [Tracing Charging Operations on page 233](#)
- [Charging Data Records on page 213](#)

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 220](#)
- [Configuring GTP Prime Peers on page 221](#)

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 219](#)
- [Configuring Transport Profiles on page 226](#)
- [Charging Services Overview on page 211](#)

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 222](#)
- [Tracing Persistent Storage Operations on page 223](#)

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
```

9. 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)
```

10. 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)
```

11. 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:

1. 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
```

2. (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
```

3. (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) |
| 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 224](#)
- [Configuring Charging on page 219](#)
- [Configuring Transport Profiles on page 226](#)
- [Charging Services Overview on page 211](#)

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 225](#)
- [Ejecting the Solid State Disk on page 225](#)
- [Installing the Solid State Disk on page 225](#)

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 222](#)
- [request system storage unified-edge charging media start on page 881](#)
- [request system storage unified-edge charging media stop on page 882](#)
- [request system storage unified-edge media eject on page 883](#)
- [request system storage unified-edge media prepare on page 884](#)

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
```

- 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
```

- 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
```

- 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)
```

- 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
```

- 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 219](#)
- [Configuring GTP Prime for Charging on page 220](#)
- [Configuring Persistent Storage on page 222](#)
- [Configuring Charging Profiles on page 231](#)
- [Charging Profiles on page 217](#)

Configuring Charging Trigger Events

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

To configure trigger profiles:

- 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
```

- 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 219](#)
 - [Configuring Charging Profiles on page 231](#)
 - [Charging Profiles on page 217](#)

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
```

4. 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 |
| 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 |

| Information Element | Information in CDRs |
|----------------------------------|---------------------------|
| user-location-information | User location information |

- Related Documentation**
- [Configuring Charging on page 219](#)
 - [Configuring Charging Profiles on page 231](#)
 - [Charging Profiles on page 217](#)

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
```

5. (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
```

6. (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
```

7. (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
```

8. (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 219](#)
 - [Charging Profiles on page 217](#)

Configuring Charging Profiles for APNs

You can configure charging profiles that apply to access point names (APNs) that are used for the default profile, home subscribers, roaming subscribers, and visiting subscribers.

To configure charging profiles for APNs:

1. Specify that you want to configure charging profiles for a particular APN.

```
[edit]  
user@host# edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-name  
charging
```

2. Specify the name of the default charging profile. The charging profile must be defined.

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

3. Specify the name of the charging profile for home subscribers roaming in other Public Land Mobile Networks (PLMNs). The charging profile must be defined.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-name charging]  
user@host# set home-profile profile-name
```

4. Specify the name of the charging profile for roaming subscribers between PLMNs. The charging profile must be defined.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-name charging]  
user@host# set roamer-profile profile-name
```

5. Specify the name of the charging profile for visiting subscribers from other PLMNs. The charging profile must be defined.

```
[edit unified-edge gateways ggsn-pgw MBG1 apn-services apns apn-name charging]  
user@host# set visitor-profile profile-name
```

6. Specify the profile selection order. You can order the selections by the charging profile sent by the RADIUS server (radius), the charging profile sent by the SGSN or Serving Gateway (serving), or the locally configured charging profile (static).

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



```
user@host# set profile-selection-order [(serving | radius | static)]
```

- Related Documentation**
- [Configuring Charging on page 219](#)
 - [Charging Profiles on page 217](#)

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 233](#)
- [Configuring the Tracing Flags on page 234](#)

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 |
| 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 219](#)

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 222](#)
 - [Configuring GTP Prime for Charging on page 220](#)
 - [Configuring Transport Profiles on page 226](#)
 - [Configuring Charging Trigger Events on page 227](#)

PART 7

Quality of Service Configuration

- [Configuring Quality of Service on page 239](#)

CHAPTER 12

Configuring Quality of Service

- [Quality of Service Overview on page 240](#)
- [Call Admission Control Overview on page 245](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 247](#)
- [Policing Subscriber Traffic on the Broadband Gateway Overview on page 248](#)
- [Applying Rewrite Rules on Mobile Interfaces Overview on page 249](#)
- [Understanding Upstream and Downstream Processing of ToS Values in GTP-U Packets on page 250](#)
- [Understanding How NQN and Upgrade Flags in PDP Contexts Affect QoS Upgrade Behavior on page 251](#)
- [Configuring QoS on the Broadband Gateway Overview on page 253](#)
- [Configuring the Maximum Number of Bearers on page 254](#)
- [Configuring Bandwidth Pools on page 255](#)
- [Configuring Preemption for Call Admission Control on page 256](#)
- [Configuring Resource Thresholds on a 4G Network on page 256](#)
- [Configuring Resource Thresholds on a 3G Network on page 258](#)
- [Configuring Resource Thresholds for 3G and 4G Networks on page 260](#)
- [Configuring a Classifier Profile for a 4G Network on page 262](#)
- [Configuring a Classifier Profile for a 3G Network on page 263](#)
- [Configuring a Classifier Profile for 3G and 4G Networks on page 264](#)
- [Configuring a CoS Policy Profile for a 4G Network on page 266](#)
- [Configuring a CoS Policy Profile for a 3G Network on page 268](#)
- [Configuring a CoS Policy Profile for 3G and 4G Networks on page 270](#)
- [Configuring a Local Policy on page 273](#)
- [Applying a Local Policy on page 274](#)
- [Configuring Ingress Rewrite Rules for a Mobile Interface on page 274](#)
- [Configuring Egress Rewrite Rules for a Mobile Interface on page 275](#)
- [Applying Ingress Rewrite Rules to a Mobile Interface on page 276](#)

- [Applying Egress Rewrite Rules to Mobile Interfaces on page 276](#)
- [Example: Configuring Quality of Service on page 277](#)

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 240](#)
- [Differentiated Services on page 240](#)
- [QoS Parameters in 3G Networks on page 241](#)
- [QoS Parameters in 4G Networks on page 242](#)
- [Aggregate Maximum Bit Rate on page 244](#)
- [Allocation and Retention Priority on page 244](#)
- [Preemption on page 244](#)

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.

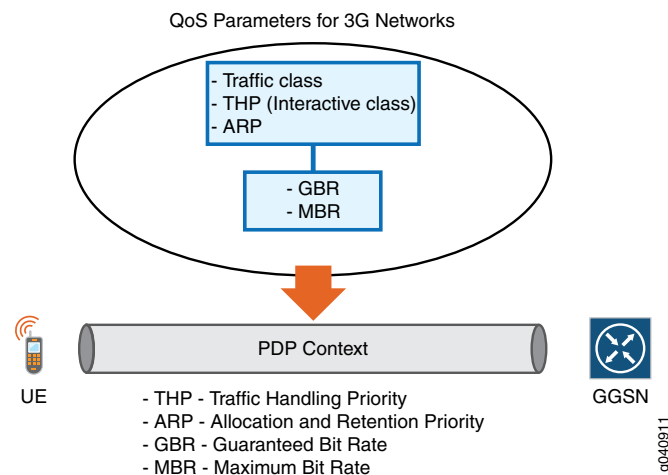
Table 35 on page 241 shows the supported traffic classes, as defined in the 3GPP standards.

Table 35: 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 33 on page 242 shows the QoS parameters that the broadband gateway evaluates to determine whether to limit, upgrade, or reject an incoming PDP context request.

Figure 33: Key QoS Parameters for PDP Context Requests



The guaranteed bit rate (GBR), shown in [Figure 33 on page 242](#), 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 33 on page 242](#), 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 36 on page 242](#) shows the supported QoS Class Identifiers and the associated set of QoS characteristics, as defined in the 3GPP standards.

Table 36: 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 36: 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.

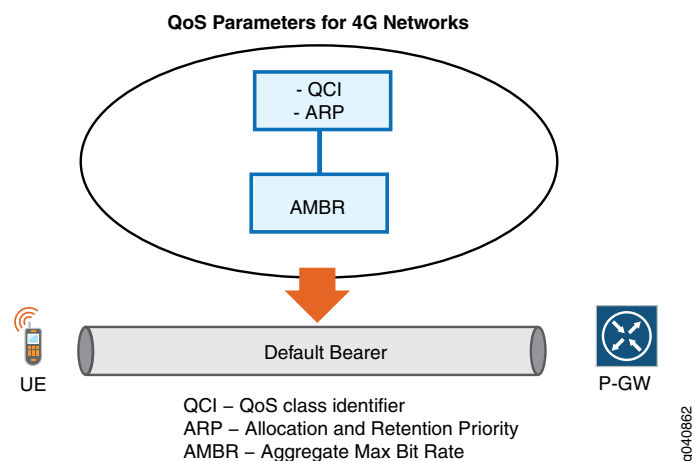
The packet error loss rate defines the percentage of higher layer packets—for example, IP packets—that are lost during periods when the network is not congested.



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 SGI interface, is carried over.

A policy profile defines the QoS treatment to be applied to default bearer requests based on the configured QoS parameters. Figure 34 on page 243 shows the QoS parameters that the broadband gateway processes to determine whether to limit, upgrade, or reject bearer requests.

Figure 34: 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 245](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 247](#)

- [Applying Rewrite Rules on Mobile Interfaces Overview on page 249](#)
- [Configuring QoS on the Broadband Gateway Overview on page 253](#)

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 245](#)
- [Managing Bandwidth on page 245](#)
- [Managing the Number of Bearers on page 246](#)
- [Managing Resource Thresholds on page 246](#)
- [Default Resource Threshold Settings on page 247](#)

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 240](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 247](#)
- [Policing Subscriber Traffic on the Broadband Gateway Overview on page 248](#)
- [Configuring QoS on the Broadband Gateway Overview on page 253](#)

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 240](#)
- [Call Admission Control Overview on page 245](#)
- [Configuring QoS on the Broadband Gateway Overview on page 253](#)

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 240](#)

- [Call Admission Control Overview on page 245](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 247](#)
- [Configuring QoS on the Broadband Gateway Overview on page 253](#)

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 240](#)
- [Call Admission Control Overview on page 245](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 247](#)
- [Configuring QoS on the Broadband Gateway Overview on page 253](#)
- [Understanding Upstream and Downstream Processing of ToS Values in GTP-U Packets on page 250](#)

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 250](#)
- [Processing of ToS Values for Downstream Subscriber Packets on page 251](#)

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 249](#)

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 35 on page 252](#) shows how negotiated QoS values are affected based on the presence of NQN or Upgrade flags in Create/Update PDP context requests.

Figure 35: 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 35 on page 252](#), 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 35 on page 252](#), 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 35 on page 252](#), 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 247](#)

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 245](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 247](#)
- [Policing Subscriber Traffic on the Broadband Gateway Overview on page 248](#)
- [Applying Rewrite Rules on Mobile Interfaces Overview on page 249](#)

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 253](#)
- [Call Admission Control Overview on page 245](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 247](#)

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 253](#)

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 253](#)
- [Call Admission Control Overview on page 245](#)
- [Class of Service \(CoS\) Policy Profile Overview on page 247](#)

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 253](#)
- [Call Admission Control Overview on page 245](#)
- [Configuring Resource Thresholds on a 3G Network on page 258](#)
- [Configuring Resource Thresholds for 3G and 4G Networks on page 260](#)
- [Example: Configuring Quality of Service on page 277](#)

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 253](#)
- [Call Admission Control Overview on page 245](#)
- [Configuring Resource Thresholds on a 4G Network on page 256](#)
- [Configuring Resource Thresholds for 3G and 4G Networks on page 260](#)
- [Example: Configuring Quality of Service on page 277](#)

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 253](#)
- [Call Admission Control Overview on page 245](#)
- [Configuring Resource Thresholds on a 4G Network on page 256](#)
- [Configuring Resource Thresholds on a 3G Network on page 258](#)
- [Example: Configuring Quality of Service on page 277](#)

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 253](#)
- [Configuring a Classifier Profile for a 3G Network on page 263](#)
- [Configuring a Classifier Profile for 3G and 4G Networks on page 264](#)
- [Example: Configuring Quality of Service on page 277](#)

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 253](#)
- [Configuring a Classifier Profile for a 4G Network on page 262](#)
- [Configuring a Classifier Profile for 3G and 4G Networks on page 264](#)
- [Example: Configuring Quality of Service on page 277](#)

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 253](#)
- [Configuring a Classifier Profile for a 4G Network on page 262](#)
- [Configuring a Classifier Profile for a 3G Network on page 263](#)
- [Example: Configuring Quality of Service on page 277](#)

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 247](#)
- [Configuring QoS on the Broadband Gateway Overview on page 253](#)
- [Configuring a CoS Policy Profile for a 3G Network on page 268](#)
- [Configuring a CoS Policy Profile for 3G and 4G Networks on page 270](#)
- [Example: Configuring Quality of Service on page 277](#)

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 247](#)
- [Configuring QoS on the Broadband Gateway Overview on page 253](#)
- [Configuring a CoS Policy Profile for a 4G Network on page 266](#)
- [Configuring a CoS Policy Profile for 3G and 4G Networks on page 270](#)
- [Example: Configuring Quality of Service on page 277](#)

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 247](#)
- [Configuring QoS on the Broadband Gateway Overview on page 253](#)
- [Configuring a CoS Policy Profile for a 4G Network on page 266](#)
- [Configuring a CoS Policy Profile for a 3G Network on page 268](#)

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 253](#)
- [Configuring the Maximum Number of Bearers on page 254](#)
- [Configuring Bandwidth Pools on page 255](#)

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 273](#)
- [Configuring the Maximum Number of Bearers on page 254](#)
- [Configuring Bandwidth Pools on page 255](#)
- [Configuring QoS on the Broadband Gateway Overview on page 253](#)

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 249](#)
 - [Configuring Egress Rewrite Rules for a Mobile Interface on page 275](#)
 - [Configuring QoS on the Broadband Gateway Overview on page 253](#)

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 249](#)
 - [Configuring QoS on the Broadband Gateway Overview on page 253](#)
 - [Configuring Ingress Rewrite Rules for a Mobile Interface on page 274](#)

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 249](#)
- [Configuring QoS on the Broadband Gateway Overview on page 253](#)
- [Applying Egress Rewrite Rules to Mobile Interfaces on page 276](#)

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 249](#)
- [Configuring QoS on the Broadband Gateway Overview on page 253](#)
- [Applying Ingress Rewrite Rules to a Mobile Interface on page 276](#)

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 277](#)
- [Overview on page 278](#)
- [Configuration on page 278](#)
- [Verification on page 310](#)

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 linternet, 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 279](#)
- [Configuring Classifier Profiles for Home Subscribers on a 4G Network on page 280](#)
- [Configuring Classifier Profiles for Roaming Subscribers on a 3G Network on page 281](#)
- [Configuring Classifier Profiles for Roaming Subscribers on a 4G Network on page 281](#)
- [Configuring Classifier Profiles for Visitor Subscribers on a 3G Network on page 282](#)
- [Configuring Classifier Profiles for Visitor Subscribers on a 4G Network on page 283](#)
- [Configuring a System-Wide Classifier Profile on page 283](#)

- [Configuring a Resource Threshold Profile for Subscribers on a 3G Network on page 285](#)
- [Configuring a Resource Threshold Profile for Subscribers on a 4G Network on page 286](#)
- [Configuring a System-Wide Resource Threshold Profile on page 288](#)
- [Configuring a CoS Policy Profile for Home Subscribers on a 3G Network on page 291](#)
- [Configuring a CoS Policy Profile for Home Subscribers on a 4G Network on page 292](#)
- [Configuring a CoS Policy Profile for Roaming Subscribers on a 3G Network on page 293](#)
- [Configuring a CoS Policy Profile for Roaming Subscribers on a 4G Network on page 294](#)
- [Configuring a CoS Policy Profile for Visiting Subscribers in a 3G Network on page 295](#)
- [Configuring a CoS Policy Profile for Visiting Subscribers in a 4G Network on page 296](#)
- [Configuring a System-Wide CoS Policy Profile on page 298](#)
- [Configuring Bandwidth Pools on page 299](#)
- [Configuring a Local Policy for 3G Networks on page 300](#)
- [Configuring a Local Policy for 4G Networks on page 301](#)
- [Configuring a System-Wide Local Policy on page 302](#)
- [Applying the Local Policies on page 303](#)
- [Configuring DSCP Ingress Rewrite Rules for IPv4 Packets on page 304](#)
- [Configuring DSCP Ingress Rewrite Rules for IPv6 Packets on page 305](#)
- [Configuring DSCP Egress Rewrite Rules for IPv4 Packets on page 306](#)
- [Configuring DSCP Egress Rewrite Rules for IPv6 Packets on page 307](#)
- [Applying Ingress Rewrite Rules to Mobile Interfaces for 3G and 4G Subscriber Traffic on page 308](#)
- [Applying Egress Rewrite Rules to Mobile Interfaces for 3G and 4G Subscriber Traffic on page 308](#)
- [Configuring the Maximum Number of Bearers on page 309](#)
- [Enabling Preemption on page 309](#)

[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:

1. 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
```

- Specify a bandwidth pool for downlink traffic.

```
[edit]
user@host# set unified-edge local-policies local_v1 dl-bandwidth-pool
bw_pool_downlink
```

- 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:

- Specify a name for the local policy.

```
[edit]
user@ggsn-pgw# edit unified-edge local-policies local_v2
```

- 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
```

- 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
```

- 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
```

- 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
```

3. At the APN level, apply the local policy for 4G subscriber traffic.

```
[edit]
user@host# set gateways ggsn-pgw MBG1 apn-services apns qosv2.com
local-policy-profile local_v2
```

Configuring DSCP Ingress Rewrite Rules for IPv4 Packets

CLI Quick Configuration To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
[edit class-of-service rewrite-rules dscp dscpv4_ingress_rw]
[set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding class af1 loss-priority
high code-point 001110]
[set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding class af1 loss-priority
low code-point 001010]
[set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding class af2 loss-priority
high code-point 010110]
[set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding class af2 loss-priority
low code-point 010010]
[set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding class af3 loss-priority
high code-point 011110]
[set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding class af3 loss-priority
low code-point 011010]
[set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding class af4 loss-priority
high code-point 100110]
[set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding class af4 loss-priority
low code-point 100010]
```

Step-by-Step Procedure To configure the ingress rewrite rules for IPv4 packets:

1. Specify a name for the ingress rewrite rules.

```
[edit]
user@host# edit class-of-service rewrite-rules dscp dscpv4_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 dscpv4_ingress_rw forwarding
class af1 loss-priority high code-point 001110
user@host# set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding
class af1 loss-priority low code-point 001010
user@host# set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding
class af2 loss-priority high code-point 010110
user@host# set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding
class af2 loss-priority low code-point 010010
user@host# set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding
class af3 loss-priority high code-point 011110
user@host# [set class-of-service rewrite-rules dscp dscpv4_ingress_rw forwarding
class af3 loss-priority low code-point 011010]
```



```

user@host# [set class-of-service rewrite-rules dscp dscp_v4_ingress_rw forwarding
class af4 loss-priority high code-point 100110
user@host# [set class-of-service rewrite-rules dscp dscp_v4_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 dscpv4_egress_rw]
[set class-of-service rewrite-rules dscp dscpv4_egress_rw forwarding class af1 loss-priority
  high code-point 001110]
[set class-of-service rewrite-rules dscp dscpv4_egress_rw forwarding class af1 loss-priority
  low code-point 001010]]
[set class-of-service rewrite-rules dscp dscpv4_egress_rw forwarding class af2 loss-priority
  high code-point 010110]
[set class-of-service rewrite-rules dscp dscpv4_egress_rw forwarding class af2 loss-priority
  low code-point 010010]
[set class-of-service rewrite-rules dscp dscpv4_egress_rw forwarding class af3 loss-priority
  high code-point 011110]
[set class-of-service rewrite-rules dscp dscpv4_egress_rw forwarding class af3 loss-priority
  low code-point 011010]
[set class-of-service rewrite-rules dscp dscpv4_egress_rw forwarding class af4 loss-priority
  high code-point 100110]
[set class-of-service rewrite-rules dscp dscpv4_egress_rw forwarding class af4 loss-priority
  low code-point 100010]
[set class-of-service rewrite-rules dscp dscpv4_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 dscpipv6_egress_rw]
[set class-of-service rewrite-rules dscp-ipv6 dscpipv6_egress_rw forwarding class af1
  loss-priority high code-point 001110]
[set class-of-service rewrite-rules dscp-ipv6 dscpipv6_egress_rw forwarding class af1
  loss-priority low code-point 001010]
[set class-of-service rewrite-rules dscp-ipv6 dscpipv6_egress_rw forwarding class af2
  loss-priority high code-point 010110]
[set class-of-service rewrite-rules dscp-ipv6 dscpipv6_egress_rw forwarding class af2
  loss-priority low code-point 010010]
[set class-of-service rewrite-rules dscp-ipv6 dscpipv6_egress_rw forwarding class af3
  loss-priority high code-point 011110]
[set class-of-service rewrite-rules dscp-ipv6 dscpipv6_egress_rw forwarding class af3
  loss-priority low code-point 011010]
[set class-of-service rewrite-rules dscp-ipv6 dscpipv6_egress_rw forwarding class af4
  loss-priority high code-point 100110]
[set class-of-service rewrite-rules dscp-ipv6 dscpipv6_egress_rw forwarding class af4
  loss-priority low code-point 100010]
[set class-of-service rewrite-rules dscp-ipv6 dscpipv6_egress_rw forwarding class be
  loss-priority low code-point 000000]
```

Step-by-Step Procedure To configure the ingress rewrite rules for IPv6 packets:

1. Specify a name for the egress rewrite rules.
2. Configure the egress rewrite rules mappings for traffic on the mobile interface.

```
[edit]
user@host# edit class-of-service rewrite-rules dscp-ipv6 dscpipv6_egress_rw
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpipv6_egress_rw
  forwarding class af1 loss-priority high code-point 001110
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpipv6_egress_rw
  forwarding class af1 loss-priority low code-point 001010
user@host# [set class-of-service rewrite-rules dscp-ipv6 dscpipv6_egress_rw
  forwarding class af2 loss-priority high code-point 010110
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpipv6_egress_rw
  forwarding class af2 loss-priority low code-point 010010
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpipv6_egress_rw
  forwarding class af3 loss-priority high code-point 011110
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpipv6_egress_rw
  forwarding class af3 loss-priority low code-point 011010
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpipv6_egress_rw
  forwarding class af4 loss-priority high code-point 100110
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpipv6_egress_rw
  forwarding class af4 loss-priority low code-point 100010
user@host# set class-of-service rewrite-rules dscp-ipv6 dscpipv6_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
dscp6_egress_rw protocol gtp-inet-both
```

```
[edit]
user@host# set class-of-service interfaces mif unit 1 rewrite-rules dscp
dscp4_egress_rw protocol gtp-inet-both
user@host# set class-of-service interfaces mif unit 1 rewrite-rules dscp
dscp6_egress_rw protocol gtp-inet-both
```

2. To apply ingress rewrite rules to change DSCPv4 and DSCPv6 values in the outer IP header of 4G subscriber packets arriving on the **qosv2.com** APN (mif.1), specify the names of the rewrite rules that you want to apply to the mobile interface.

```
[edit]
user@host# set class-of-service interfaces mif unit 1 rewrite-rules dscp
dscp4_egress_rw protocol gtp-inet-both
user@host# set class-of-service interfaces mif unit 1 rewrite-rules dscp
dscp6_egress_rw protocol gtp-inet-both
```

Configuring the Maximum Number of Bearers

Step-by-Step Procedure You configure the maximum bearers to specify an upper limit on the number of bearers allowed at the system level and, optionally, the APN level. When the total number of active bearers at the system level or APN level reaches the maximum configured limit, the broadband gateway rejects new bearer requests.

To configure the maximum number of active bearers:

1. Configure the number of maximum bearers allowed at the system level.

```
[edit]
user@host# set unified-edge gateways ggsn-pgw MBG1 maximum-bearers 5000000
```

Enabling Preemption

Step-by-Step Procedure You can enable preemption at the system level to enable the preemption capability indicator (PCI) and preemption vulnerability indicator (PVI) flags. Preemption is disabled by default.

To enable preemption or both 3G (GTPv1) and 4G (GTPv2) subscriber traffic:

1. Configure preemption at the system level.

```
[edit]
```

```
user@host# set unified-edge gateways ggsn-pgw MBG1 preemption enable
```

Verification

To display QoS statistics for 3G and 4G subscriber packets to verify that the QoS configuration on the broadband gateway is working properly, you can perform the following tasks:

- [Display QoS Statistics for 4G Subscriber Packets with a Specified Allocation Retention Priority](#) on page 310
- [Display 4G Subscriber Information for Traffic Marked with a Specified QoS Class Identifier](#) on page 311
- [Display 3G Subscriber Information for Traffic Marked with the Specified Traffic Class](#) on page 311
- [Display the Requested and Negotiated QoS Parameters for Mobile Subscribers](#) on page 312

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 240](#)
 - [Call Admission Control Overview on page 245](#)
 - [Class of Service \(CoS\) Policy Profile Overview on page 247](#)
 - [Policing Subscriber Traffic on the Broadband Gateway Overview on page 248](#)
 - [Configuring QoS on the Broadband Gateway Overview on page 253](#)

PART 8

Maintenance

- [Maintenance Mode on page 317](#)

CHAPTER 13

Maintenance Mode

- [Mobility Maintenance Mode Overview on page 318](#)
- [Changing a GTP Interface Address on page 319](#)
- [Deleting a GTP Interface on page 320](#)
- [Modifying an Access Point Name on page 322](#)
- [Configuring the Mobile Interface of an Access Point Name on page 323](#)
- [Deleting an Access Point Name on page 325](#)
- [Changing a Charging Profile on page 326](#)
- [Changing a Transport Profile on page 327](#)
- [Changing a Trigger Profile on page 329](#)
- [Deleting a Charging Profile on page 330](#)
- [Changing a Call Detail Record Profile in a Charging Profile on page 331](#)
- [Changing Address Attributes in the Mobile Address Pool on page 332](#)
- [Deleting a Mobile Address Pool on page 334](#)
- [Example: Changing Access Point Name Values on page 335](#)
- [Example: Deleting an APN on page 336](#)
- [Example: Changing a Charging Profile on page 337](#)
- [Example: Changing a Transport Profile on page 339](#)
- [Example: Changing Mobility Pool Attributes on page 340](#)
- [Example: Deleting a Mobility Address Pool on page 346](#)
- [Example: Modifying Mobile Interface Parameters on page 347](#)

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 319](#)
- [Deleting a GTP Interface on page 320](#)
- [Modifying an Access Point Name on page 322](#)
- [Configuring the Mobile Interface of an Access Point Name on page 323](#)
- [Deleting an Access Point Name on page 325](#)
- [Changing a Charging Profile on page 326](#)
- [Deleting a Charging Profile on page 330](#)
- [Changing a Transport Profile on page 327](#)

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 318](#)
- [Deleting a GTP Interface on page 320](#)

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 318](#)
- [Changing a GTP Interface Address on page 319](#)

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 318](#)
- [Configuring the Mobile Interface of an Access Point Name on page 323](#)
- [Deleting an Access Point Name on page 325](#)

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 318](#)
- [Example: Changing Access Point Name Values on page 335](#)
- [Deleting an Access Point Name on page 325](#)

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 318](#)
- [Configuring the Mobile Interface of an Access Point Name on page 323](#)
- [Example: Changing Access Point Name Values on page 335](#)

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
```

- 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.

- 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
```

- 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
```

- 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 318](#)
- [Changing a Transport Profile on page 327](#)
- [Changing a Trigger Profile on page 329](#)
- [Deleting a Charging Profile on page 330](#)
- [Changing a Call Detail Record Profile in a Charging Profile on page 331](#)

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:

- Enter configuration mode in the CLI.

```
user@host> configure
```

- 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
```

- 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 318](#)
- [Changing a Charging Profile on page 326](#)
- [Changing a Trigger Profile on page 329](#)
- [Deleting a Charging Profile on page 330](#)
- [Changing a Call Detail Record Profile in a Charging Profile on page 331](#)

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 318](#)
- [Changing a Charging Profile on page 326](#)

- [Changing a Transport Profile on page 327](#)
- [Deleting a Charging Profile on page 330](#)
- [Changing a Call Detail Record Profile in a Charging Profile on page 331](#)

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 318](#)
- [Changing a Charging Profile on page 326](#)
- [Changing a Transport Profile on page 327](#)
- [Changing a Trigger Profile on page 329](#)
- [Changing a Call Detail Record Profile in a Charging Profile on page 331](#)

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 318](#)
- [Changing a Charging Profile on page 326](#)
- [Changing a Transport Profile on page 327](#)
- [Changing a Trigger Profile on page 329](#)
- [Deleting a Charging Profile on page 330](#)

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 318](#)
- [Deleting a Mobile Address Pool on page 334](#)

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 332](#)

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 318](#)
 - [Changing Address Attributes in the Mobile Address Pool on page 332](#)

Example: Changing Access Point Name Values

- [Requirements on page 335](#)
- [Overview on page 335](#)
- [Configuration on page 335](#)

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 318](#)
- [Modifying an Access Point Name on page 322](#)

Example: Deleting an APN

- [Requirements on page 336](#)
- [Overview on page 336](#)
- [Configuration on page 336](#)

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 318](#)
- [Deleting an Access Point Name on page 325](#)

Example: Changing a Charging Profile

This example shows how to change a charging profile using maintenance mode.

- [Requirements on page 337](#)
- [Overview on page 338](#)
- [Configuration on page 338](#)

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 318](#)
- [Changing a Charging Profile on page 326](#)

Example: Changing a Transport Profile

This example shows how to change a transport profile using maintenance mode.

- [Requirements on page 339](#)
- [Overview on page 339](#)
- [Configuration on page 339](#)

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 318](#)
- [Changing a Transport Profile on page 327](#)

Example: Changing Mobility Pool Attributes

- [Requirements on page 340](#)
- [Overview on page 340](#)
- [Configuration on page 340](#)

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 318](#)
- [Changing Address Attributes in the Mobile Address Pool on page 332](#)

Example: Deleting a Mobility Address Pool

- [Requirements on page 346](#)
- [Example of Deleting a Mobility Address Pool on page 346](#)
- [Configuration on page 346](#)

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 318](#)
 - [Deleting a Mobile Address Pool on page 334](#)

Example: Modifying Mobile Interface Parameters

- [Requirements on page 348](#)
- [Overview on page 348](#)
- [Configuration on page 348](#)

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 348](#)
- [Changing the Mobile Interface for an Access Point Name \(APN\) on page 349](#)

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-ggsn;
}
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 318](#)
- [Deleting a Mobile Address Pool on page 334](#)

PART 9

Monitoring and Troubleshooting

- [Monitoring on page 353](#)
- [Troubleshooting on page 381](#)

Monitoring

- [Monitoring the Mobile Environment - Key Performance Indicators on page 353](#)
- [Monitoring Resources on page 354](#)
- [Monitoring GTP Signaling on page 354](#)
- [Monitoring Session Status on page 355](#)
- [Monitoring CPU Indicators on page 356](#)
- [Monitoring Memory Indicators on page 357](#)
- [Monitoring Charging Gateways on page 357](#)
- [Monitoring Data Path Measurements on page 359](#)
- [Monitoring Call Rate Statistics on page 359](#)
- [Monitoring Data Rate Statistics on page 359](#)
- [Tracing Control Packets on page 362](#)
- [How to Trace Data Packets from Gn to Gi Interfaces on page 366](#)
- [Trace Data Packets from Gi to Gn Interfaces on page 370](#)
- [How to Verify Charging Statistics Processing on page 377](#)

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 359](#)
- [Monitoring Data Path Measurements on page 359](#)
- [Monitoring Session Status on page 355](#)
- [Monitoring GTP Signaling on page 354](#)

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 353](#)
 - [Monitoring Resources on page 354](#)

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 353](#)
 - [Monitoring Resources on page 354](#)

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 353](#)
 - [Monitoring Resources on page 354](#)
 - [Monitoring Memory Indicators on page 357](#)

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-resourcetbl
```

- Related Documentation**
- [Monitoring the Mobile Environment - Key Performance Indicators on page 353](#)
 - [Monitoring Resources on page 354](#)
 - [Monitoring CPU Indicators on page 356](#)

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 353](#)
 - [Monitoring Resources on page 354](#)

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 353](#)
 - [Monitoring Resources on page 354](#)

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 353](#)
 - [Monitoring Resources on page 354](#)

Tracing Control Packets

- [Requirements on page 362](#)
- [Tracing Control Packets on page 362](#)
- [Configuration on page 366](#)

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 366](#)

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 353](#)
 - [Monitoring Resources on page 354](#)

How to Trace Data Packets from Gn to Gi Interfaces

- [Requirements on page 366](#)
- [Tracing Data Packets on page 366](#)
- [Configuration on page 366](#)

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 366](#)

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_frags_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 353](#)
- [Monitoring Resources on page 354](#)

Trace Data Packets from Gi to Gn Interfaces

- [Requirements on page 370](#)
- [Tracing Data Packets on page 370](#)
- [Configuration on page 371](#)

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 371](#)

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 353](#)
- [Monitoring Resources on page 354](#)
- [How to Trace Data Packets from Gn to Gi Interfaces on page 366](#)

How to Verify Charging Statistics Processing

- [Requirements on page 377](#)
- [Verifying Packet Forwarding Engine Charging Statistics Are Processing Properly on page 377](#)
- [Configuration on page 377](#)

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 378](#)

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 353](#)
 - [Monitoring Resources on page 354](#)

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 381](#)
- [Troubleshooting Multilevel Overload Protection on page 381](#)
- [Responding to an Overload on page 382](#)
- [Monitoring GTP Signaling on page 382](#)
- [Troubleshooting Alarms, Logs, and Traps on page 383](#)
- [Troubleshooting Admission Control on page 385](#)
- [Monitoring AAA Metrics on page 387](#)

[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 382](#)

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 353](#)
 - [Monitoring Resources on page 354](#)

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 395](#)

CHAPTER 16

Example Configurations

- [Example: Simple Unified Edge Configuration on page 395](#)
- [Example: Configuring MobileNext Broadband Gateway on page 403](#)
- [Example: Configuring MobileNext Broadband Gateway with Provider Edge Functionality on page 431](#)
- [Example: Configuring NAT on page 440](#)

Example: Simple Unified Edge Configuration

This example describes how to configure a simple unified edge, and consists of the following sections:

- [Requirements on page 395](#)
- [Overview and Topology on page 395](#)
- [Configuration on page 396](#)
- [Verification on page 402](#)

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 37 on page 396](#) shows the MobileNext Broadband Gateway components used in this solution.

Table 37: 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 397](#)
- [Configuring the Interface to the Gn Side on page 398](#)
- [Configuring the Mobile Interface Units for Mobility Support on page 399](#)
- [Configuring the Address Pool for Assigning IP Addresses to the User Equipment on page 400](#)
- [Configuring the GGSN Parameters on page 401](#)

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 {
              range {
                r1 {
                  low 29.0.0.1;
                  high 29.255.255.254;
                }
              }
            }
          }
        }
      }
    }
  }
}
```



```

    }
    default-pool;
  }
}

```

Configuring the GGSN Parameters

CLI Quick Configuration To quickly configure the GGSN parameters, copy the following statements and paste them into the router terminal window:

```

[edit unified-edge gateways ggsn-pgw PGW]
set home-plmn mcc 421 mnc 342
edit gtp
set gn interface lo0.0 v4-address 99.1.1.1

```

Step-by-Step Procedure To define a broadband gateway GTP configuration, from the customer edge to the provider network:

1. Define the broadband gateway as P-GW.

```

user@host# edit unified-edge gateways ggsn-pgw PGW

```
2. Define the home public land mobile network (HPLMN), mobile country code (MCC), and mobile network code (MNC).

```

[edit unified-edge gateways ggsn-pgw PGW]
user@host# set home-plmn mcc 421 mnc 342

```
3. Configure the GTP settings.

```

user@host# edit unified-edge gateways ggsn-pgw PGW gtp

```
4. Configure the Gn interface for receiving GTP-C and GTP-U packets on the GGSN to use the loopback interface and IP address specified.

```

[edit unified-edge gateways ggsn-pgw PGW gtp ]
user@host# set gn interface lo0.0 v4-address 99.1.1.1

```

Results Check the results of the configuration:

```

user@host# edit unified-edge
user@host# show
unified-edge {
  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 402](#)
- [Verifying the Gateway Configuration on page 402](#)

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 186](#)
- [Configuring a Local Policy on page 273](#)
- [Configuring GTP Trace Options on page 207](#)

- [Configuring GTP Services on the Gn Interface on page 196](#)
- [Configuring a Loopback Interface for Transport of GTP Packets on page 188](#)

Example: Configuring MobileNext Broadband Gateway

This example describes how to configure the MobileNext Broadband Gateway without any provider edge functionality.

- [Requirements on page 403](#)
- [Overview on page 403](#)
- [Configuration on page 404](#)
- [Verification on page 421](#)

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 38: Components of the Broadband Gateway

| Property | Settings | Description |
|----------------------------------|--|--|
| Loopback address | lo0 11.11.11.1/32 | Identifies the device for communications. |
| 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). |

Table 38: Components of the Broadband Gateway (*continued*)

| Property | Settings | Description |
|---------------------------|--|---|
| 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 405](#)
- [Configuring the IPv4 Interfaces on page 406](#)
- [Enabling IS-IS on page 407](#)
- [Enabling MPLS and RSVP Routing on page 408](#)
- [Configuring BGP on page 409](#)
- [Enabling the Routing Instance for the Layer 3 VPN on page 409](#)

- [Configuring RADIUS Servers on page 410](#)
- [Configuring DHCP Proxy Clients on page 410](#)
- [Enabling the APN Configuration on page 411](#)
- [Configuring Offline Charging on page 414](#)
- [Configuring GTP Services on page 418](#)
- [Configuring AAA on page 419](#)
- [Configuring APN Parameters on page 420](#)

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
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
  wireless-juniper1 family inet network 100.103.0.0/16 range r3 high 100.103.255.255
set routing-instances VRF-wireless1.juniper.net access address-assignment mobile-pools
  wireless-juniper1 family inet network 100.104.0.0/16 range r4 low 100.104.0.0

```

[illegible]

```

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 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 gtp transport-protocol tcp
set unified-edge gateways ggsn-pgw MBG1 charging gtp version v0
set unified-edge gateways ggsn-pgw MBG1 charging gtp header-type long

```

```

set unified-edge gateways ggsn-pgw MBG1 charging gtp peer local_cgw
  destination-ipv4-address 42.42.0.2
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer local_cgw source-interface
  lo0.2
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer local_cgw source-interface
  ipv4-address 11.11.11.1
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer local_cgw destination-port
  3386
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer local_cgw transport-protocol
  tcp
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer local_cgw n3-requests 1
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer local_cgw t3-response 3
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer local_cgw header-type long
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer local_cgw
  pending-queue-size 1000
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer my_cgf
  destination-ipv4-address 41.41.0.2
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer my_cgf source-interface
  lo0.12
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer my_cgf source-interface
  ipv4-address 11.11.11.1
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer my_cgf destination-port
  3386
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer my_cgf transport-protocol
  tcp
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer my_cgf n3-requests 1
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer my_cgf t3-response 5
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer my_cgf header-type long
set unified-edge gateways ggsn-pgw MBG1 charging gtp peer my_cgf pending-queue-size
  1000

```

Step-by-Step Procedure

To configure the offline charging profile:

1. Create the routing instances for charging. CHR-VRF is for the external charging gateway and CHR-VRF-Local is for persistent local storage.


```

[edit]
user@pe1# set routing-instances CHR-VRF instance-type vrf
user@pe1# set routing-instances CHR-VRF interface lo0.12
user@pe1# set routing-instances CHR-VRF route-distinguisher 10.102.32.59:1000
user@pe1# set routing-instances CHR-VRF vrf-target target:5000:1000
user@pe1# set routing-instances CHR-VRF vrf-table-label
user@pe1# set routing-instances CHR-VRF-Local instance-type virtual-router
user@pe1# set routing-instances CHR-VRF-Local interface ge-0/0/6.0
user@pe1# set routing-instances CHR-VRF-Local interface lo0.2

```
2. Configure charging for the GGSN called MBG1.


```

[edit]
user@pe1# edit unified-edge gateways ggsn-pgw MBG1 charging

```
3. Specify the global GTP Prime properties to transmit CDRs to the external charging gateway.


```

[edit unified-edge gateways ggsn-pgw MBG1 charging]
user@pe1# set gtp transport-protocol tcp
user@pe1# set gtp version v0

```



```
user@pe1# set gtp header-type long
```

4. Specify the GTP Prime properties for the GTP Prime peers.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging]
user@pe1# set gtp peer local_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_cgf destination-ipv4-address 41.41.0.2
user@pe1# set gtp peer my_cgf source-interface lo0.12
user@pe1# set gtp peer my_cgf source-interface ipv4-address 11.11.11.1
user@pe1# set gtp peer my_cgf destination-port 3386
user@pe1# set gtp peer my_cgf transport-protocol tcp
user@pe1# set gtp peer my_cgf n3-requests 1
user@pe1# set gtp peer my_cgf t3-response 5
user@pe1# set gtp peer my_cgf header-type long
user@pe1# set gtp peer my_cgf pending-queue-size 1000
```

5. Configure local persistent storage of the CDRs.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging]
user@pe1# set local-persistent-storage-options file-age 60
user@pe1# set local-persistent-storage-options file-format raw-asn
user@pe1# set local-persistent-storage-options disk-space-policy water-mark-level1
percentage 70
user@pe1# set local-persistent-storage-options disk-space-policy water-mark-level2
percentage 80
user@pe1# set local-persistent-storage-options disk-space-policy water-mark-level3
percentage 90
```

6. Configure the transport, trigger, and CDR profiles referenced by the charging profile for offline charging.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging]
user@pe1# set transport-profiles CGW-trans-pro-1 offline charging-gateways
cdr-release r7
user@pe1# set transport-profiles CGW-trans-pro-1 offline charging-gateways
peer-order peer my_cgf
user@pe1# set transport-profiles CGW-trans-pro-1 offline charging-gateways
peer-order peer local_cgw
user@pe1# set transport-profiles CGW-trans-pro-1 offline charging-gateways
switch-back-time 1
user@pe1# set transport-profiles trans-wireless1.juniper.net offline
charging-gateways cdr-release r7
user@pe1# set transport-profiles trans-wireless1.juniper.net offline
charging-gateways persistent-storage-order local-storage
user@pe1# set trigger-profiles CGW-trig-pro-1 offline volume-limit 1048576
user@pe1# set trigger-profiles CGW-trig-pro-1 offline volume-limit direction both
user@pe1# set trigger-profiles trigr-wireless1.juniper.net offline volume-limit 1048576
user@pe1# set trigger-profiles trigr-wireless1.juniper.net offline volume-limit direction
uplink
user@pe1# set cdr-profiles cdr-wireless1.juniper.net enable-reduced-partial-cdrs
```

7. Configure the charging profile. The CGW-chr-pro-1 charging profile is used for the external charging gateway, while the chr-wireless1.juniper.net charging profile is used for local persistent storage.

```
[edit unified-edge gateways ggsn-pgw MBG1 charging]
user@pe1# set charging-profiles CGW-chr-pro-1 profile-id 2
user@pe1# set charging-profiles CGW-chr-pro-1 transport-profile CGW-trans-pro-1
user@pe1# set charging-profiles CGW-chr-pro-1 trigger-profile CGW-trig-pro-1
user@pe1# set charging-profiles chr-wireless1.juniper.net profile-id 1
user@pe1# set charging-profiles chr-wireless1.juniper.net transport-profile
trans-wireless1.juniper.net
user@pe1# set charging-profiles chr-wireless1.juniper.net cdr-profile
cdr-wireless1.juniper.net
user@pe1# set charging-profiles chr-wireless1.juniper.net trigger-profiles
trigr-wireless1.juniper.net
user@pe1# set charging-profiles chr-wireless1.juniper.net trigger-profile
trigr-wireless1.juniper.net
```

Configuring GTP Services

CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge gateways ggsn-pgw MBG1 gtp gn interface lo0.1
set unified-edge gateways ggsn-pgw MBG1 gtp gn interface v4-address 11.11.11.1
set unified-edge gateways ggsn-pgw MBG1 gtp gn n3-requests 3
set unified-edge gateways ggsn-pgw MBG1 gtp gn t3-response 3
set unified-edge gateways ggsn-pgw MBG1 gtp gn echo-interval 60
set unified-edge gateways ggsn-pgw MBG1 gtp gn path-management enable
set unified-edge gateways ggsn-pgw MBG1 gtp gp interface lo0.1
set unified-edge gateways ggsn-pgw MBG1 gtp gp interface v4-address 11.11.11.1
set unified-edge gateways ggsn-pgw MBG1 gtp gp n3-requests 3
set unified-edge gateways ggsn-pgw MBG1 gtp gp t3-response 3
set unified-edge gateways ggsn-pgw MBG1 gtp gp echo-interval 60
set unified-edge gateways ggsn-pgw MBG1 gtp gp path-management enable
set unified-edge gateways ggsn-pgw MBG1 gtp s5 interface lo0.1
set unified-edge gateways ggsn-pgw MBG1 gtp s5 interface v4-address 11.11.11.1
set unified-edge gateways ggsn-pgw MBG1 gtp s5 n3-requests 3
set unified-edge gateways ggsn-pgw MBG1 gtp s5 t3-response 3
set unified-edge gateways ggsn-pgw MBG1 gtp s5 echo-interval 60
set unified-edge gateways ggsn-pgw MBG1 gtp s5 path-management enable
set unified-edge gateways ggsn-pgw MBG1 gtp s8 interface lo0.1
set unified-edge gateways ggsn-pgw MBG1 gtp s8 interface v4-address 11.11.11.1
set unified-edge gateways ggsn-pgw MBG1 gtp s8 n3-requests 3
set unified-edge gateways ggsn-pgw MBG1 gtp s8 t3-response 3
set unified-edge gateways ggsn-pgw MBG1 gtp s8 echo-interval 60
set unified-edge gateways ggsn-pgw MBG1 gtp s8 path-management enable
```

Step-by-Step Procedure

To configure GTP services:

1. Configure the GTP services for the GGSN called MBG1.

```
[edit]
user@pe1# edit unified-edge gateways ggsn-pgw MBG1 gtp
```

2. Configure GTP services for the Gn, Gp, S5, and S8 interfaces with path management enabled. The same address must be specified for all addresses.

```
[edit unified-edge gateways ggsn-pgw MBG1 gtp]
user@pe1# set gn interface lo0.1
user@pe1# set gn interface v4-address 11.11.11.1
user@pe1# set gn n3-requests 3
user@pe1# set gn t3-response 3
user@pe1# set gn echo-interval 60
user@pe1# set gn path-management enable
user@pe1# set gp interface lo0.1
user@pe1# set gp interface v4-address 11.11.11.1
user@pe1# set gp n3-requests 3
user@pe1# set gp t3-response 3
user@pe1# set gp echo-interval 60
user@pe1# set gp path-management enable
user@pe1# set s5 interface lo0.1
user@pe1# set s5 interface v4-address 11.11.11.1
user@pe1# set s5 n3-requests 3
user@pe1# set s5 t3-response 3
user@pe1# set s5 echo-interval 60
user@pe1# set s5 path-management enable
user@pe1# set s8 interface lo0.1
user@pe1# set s8 interface v4-address 11.11.11.1
user@pe1# set s8 n3-requests 3
user@pe1# set s8 t3-response 3
user@pe1# set s8 echo-interval 60
user@pe1# set s8 path-management enable
```

Configuring AAA

CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set unified-edge aaa mobile-profiles aaa_profile radius authentication network-element
radius_ne
set unified-edge aaa mobile-profiles aaa_profile radius accounting network-element
radius_ne
set unified-edge aaa mobile-profiles aaa_profile radius options nas-ip-address 11.11.11.1
set unified-edge aaa mobile-profiles aaa_profile radius attributes exclude calling-station-id
access-request
set unified-edge aaa mobile-profiles aaa_profile radius attributes exclude event-time-stamp
accounting-start
```

Step-by-Step Procedure

To configure AAA profiles:

1. Configure the AAA profile called `aaa_profile` for the broadband gateway.

```
[edit]
user@pe1# edit unified-edge aaa mobile-profiles aaa_profile
```

2. Specify the RADIUS authentication and accounting settings for the profile.

```
[edit unified-edge aaa mobile-profiles aaa_profile]
user@pe1# set radius authentication network-element radius_ne
```

```
user@pe1# set radius accounting network-element radius_ne
```

3. Specify the RADIUS options.

```
[edit unified-edge aaa mobile-profiles aaa_profile]  
user@pe1# set radius options nas-ip-address 11.11.11.1
```

4. Specify the RADIUS attributes to exclude from the message type.

```
[edit unified-edge aaa mobile-profiles aaa_profile]  
user@pe1# set radius attributes exclude calling-station-id access-request  
user@pe1# set radius attributes exclude event-time-stamp accounting-start
```

Configuring APN Parameters

CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]  
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless1.juniper.net apn-type  
real  
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless1.juniper.net  
apn-data-type ipv4  
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless1.juniper.net  
mobile-interface mif.1  
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless1.juniper.net  
address-assignment local  
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless1.juniper.net  
address-assignment inet-pool pool wireless-juniper1  
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless1.juniper.net  
session-timeout 2  
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless1.juniper.net  
idle-timeout 60  
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless1.juniper.net charging  
default-charging-profile chr-wireless1.juniper.net  
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless1.juniper.net  
selection-mode from-ms  
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless2.juniper.net apn-type  
real  
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless2.juniper.net  
apn-data-type ipv4  
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless2.juniper.net  
mobile-interface mif.2  
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless2.juniper.net  
address-assignment local  
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless2.juniper.net  
address-assignment inet-pool pool wireless-juniper1  
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless2.juniper.net  
address-assignment dhcpv4-proxy-client-profile logical-system default routing-instance  
DHCP profile-name dhcp-1  
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless2.juniper.net  
session-timeout 2  
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless2.juniper.net  
idle-timeout 60  
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless2.juniper.net  
aaa-profile aaa_profile
```

```

set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless2.juniper.net charging
default-charging-profile CGW-chr-pro-1
set unified-edge gateways ggsn-pgw MBG1 apn-services apns wireless2.juniper.net
selection-mode from-ms

```

Step-by-Step Procedure

To configure APN services:

1. Configure the APN services for the GGSN called MBG1.

```

[edit]
user@pe1# edit unified-edge gateways ggsn-pgw MBG1 apn-services

```
2. Configure the wireless1.juniper.net APN used for the mif.1 interface. This APN uses the wireless-juniper1 IP pool for address assignment and chr-wireless1.juniper.net as the default charging profile.

```

[edit unified-edge gateways ggsn-pgw MBG1 apn-services]
user@pe1# set apn wireless1.juniper.net apn-type real
user@pe1# set apn wireless1.juniper.net apn-data-type ipv4
user@pe1# set apn wireless1.juniper.net mobile-interface mif.1
user@pe1# set apn wireless1.juniper.net address-assignment local
user@pe1# set apn wireless1.juniper.net address-assignment inet-pool pool
wireless-juniper1
user@pe1# set apn wireless1.juniper.net session-timeout 2
user@pe1# set apn wireless1.juniper.net idle-timeout 60
user@pe1# set apn wireless1.juniper.net charging default-charging-profile
chr-wireless1.juniper.net
user@pe1# set apn wireless1.juniper.net selection-mode from-ms

```
3. Configure the wireless2.juniper.net APN used for the mif.2 interface. This APN uses the wireless-juniper1 IP pool or dhcpv4-proxy-client-profile for address assignment. This APN uses aaa_profile as the AAA profile and CGW-chr-pro-1 as the default charging profile.

```

[edit unified-edge gateways ggsn-pgw MBG1 apn-services]
user@pe1# set apn wireless2.juniper.net apn-type real
user@pe1# set apn wireless2.juniper.net apn-data-type ipv4
user@pe1# set apn wireless2.juniper.net mobile-interface mif.2
user@pe1# set apn wireless2.juniper.net address-assignment local
user@pe1# set apn wireless2.juniper.net address-assignment inet-pool pool
wireless-juniper1
user@pe1# set apn wireless2.juniper.net address-assignment
dhcpv4-proxy-client-profile logical-system default routing-instance DHCP
profile-name
user@pe1# set apn wireless2.juniper.net session-timeout 2
user@pe1# set apn wireless2.juniper.net idle-timeout 60
user@pe1# set apn wireless2.juniper.net aaa-profile aaa_profile
user@pe1# set apn wireless2.juniper.net charging default-charging-profile
CGW-chr-pro-1
user@pe1# set apn wireless2.juniper.net selection-mode from-ms

```

Verification

Verifying MPLS LSP Status

Purpose Verify the MPLS LSP status for GGSN initiation.

Action user@pe1> show mpls lsp

Ingress LSP: 1 sessions

| To | From | State | Rt | P | ActivePath | LSPName |
|--------------|--------------|-------|----|---|------------|--------------|
| 10.255.28.17 | 10.102.32.59 | Up | 0 | * | | PE-1-to-PE-2 |

Total 1 displayed, Up 1, Down 0

Egress LSP: 1 sessions

| To | From | State | Rt | Style | Labelin | Labelout | LSPName |
|--------------|--------------|-------|----|-------|---------|----------|----------------|
| 10.102.32.59 | 10.255.28.17 | Up | 0 | 1 FF | 0 | | - PE-2-to-PE-1 |

Total 1 displayed, Up 1, Down 0

Transit LSP: 0 sessions

Total 0 displayed, Up 0, Down 0

Meaning The `show mpls lsp` command displays information about the configured label-switched paths, including the destination address.

Verifying Layer 3 VPN Status

Purpose Verify Layer 3 VPN status and routes for GGSN initiation and successful call establishment.

Action user@pe1> show route table VRF-wireless1.juniper.net

VRF-wireless1.juniper.net.inet.0: 14 destinations, 14 routes (14 active, 0 holddown, 0 hidden)

+ = Active Route, - = Last Active, * = Both

```

11.11.11.1/32      *[Direct/0] 01:08:14
                   > via lo0.10
55.55.0.0/16      *[BGP/170] 00:15:55, localpref 100, from 10.255.28.17
                   AS path: I
                   > to 33.55.0.2 via ge-5/3/0.0, label-switched-path PE-1-to-PE-2
100.104.172.0/22  *[Anchor/7] 00:04:53
                   Private indexed

100.104.176.0/22  *[Anchor/7] 00:04:52
                   Private indexed
100.104.180.0/22  *[Anchor/7] 00:04:51
                   Private indexed
100.105.20.0/22   *[Anchor/7] 00:04:53
                   Private indexed
100.105.24.0/22   *[Anchor/7] 00:04:52
                   Private indexed
100.105.28.0/22   *[Anchor/7] 00:04:51
                   Private indexed
100.105.32.0/22   *[Anchor/7] 00:04:50
                   Private indexed
100.105.36.0/22   *[Anchor/7] 00:04:50
                   Private indexed
run show unified-edge ggsn-pgw resource-manager clients | no-more
100.105.40.0/22   *[Anchor/7] 00:04:49
                   Private indexed
100.105.136.0/22  *[Anchor/7] 00:04:50
                   Private indexed
100.105.140.0/22  *[Anchor/7] 00:04:50
                   Private indexed
100.105.144.0/22  *[Anchor/7] 00:04:49
                   Private indexed

```

Meaning The `show route table` command verifies the Layer 3 VPN configuration by displaying the VRF table for the specified VRF.

Verifying Session DPCs and Interface DPCs Initialization

Purpose Verify the initialization of session DPCs and interface DPCs for GGSN initiation.

Action

```

user@pe1> show chassis fpc pic-status
Slot 0  Online      MPC Type 2 3D EQ
  PIC 0  Online      10x 1GE(LAN) SFP
  PIC 1  Online      10x 1GE(LAN) SFP
  PIC 2  Online      10x 1GE(LAN) SFP
  PIC 3  Online      10x 1GE(LAN) SFP
Slot 1  Online      MS-DPC EM
  PIC 0  Online      MS-DPC PIC
  PIC 1  Online      MS-DPC PIC
Slot 2  Online      MPC Type 2 3D EQ
  PIC 0  Online      10x 1GE(LAN) SFP
  PIC 1  Online      10x 1GE(LAN) SFP
  PIC 2  Online      10x 1GE(LAN) SFP
  PIC 3  Online      10x 1GE(LAN) SFP
Slot 3  Online      MS-DPC EM
  PIC 0  Online      MS-DPC PIC
  PIC 1  Online      MS-DPC PIC
Slot 4  Online      MPC Type 2 3D EQ
  PIC 0  Online      2x 10GE XFP
  PIC 1  Online      2x 10GE XFP
  PIC 2  Online      10x 1GE(LAN) SFP
  PIC 3  Online      10x 1GE(LAN) SFP
Slot 5  Online      MPC Type 2 3D EQ
  PIC 0  Online      10x 1GE(LAN) SFP
  PIC 1  Online      10x 1GE(LAN) SFP
  PIC 2  Online      10x 1GE(LAN) SFP
  PIC 3  Online      10x 1GE(LAN) SFP

user@pe1> show unified-edge ggsn-pgw resource-manager clients
Client      State      Role      Type
apfe-0/1    In-Service RMS_PRIMARY RCM-PFE
apfe-0/0    In-Service RMS_PRIMARY RCM-PFE
ms-1/0      In-Service RMS_PRIMARY RCM-SP
ms-1/1      In-Service RMS_PRIMARY RCM-SP
apfe-2/1    In-Service RMS_SECONDARY RCM-PFE
apfe-2/0    In-Service RMS_SECONDARY RCM-PFE
ms-3/0      In-Service RMS_SECONDARY RCM-SP
ms-3/1      In-Service RMS_SECONDARY RCM-SP
apfe-4/1    In-Service RMS_PRIMARY RCM-PFE
apfe-4/0    In-Service RMS_PRIMARY RCM-PFE
apfe-5/1    In-Service RMS_SECONDARY RCM-PFE
apfe-5/0    In-Service RMS_SECONDARY RCM-PFE

```

Meaning The `show chassis fpc pic-status` command lists the PIC status. It shows that the DPCs are initialized if the status is Online.

The `show unified-edge ggsn-pgw resource-manager clients` command lists the state for resource manager clients. It displays the In-Service state to indicate that the DPCs are initialized.

Verifying Broadband Gateway Status

Purpose Verify the status and statistics on the broadband gateway for GGSN initiation, call establishment, and Gn-to-Gi connectivity across the MPLS core.

Action

```

user@pe1> show unified-edge ggsn-pgw status
  Mobile gateway status:
    Active Subscribers      :          180
    Active Sessions        :          180
    Active Bearers          :          180
    CPU Load (%)            :           0
    Memory Load (%)         :          27

user@pe1> show unified-edge ggsn-pgw statistics
Control plane statistics:
  Session establishment attempts:      200180
  Successful session establishments:    200180
  MS/peer initiated session deactivations: 199611
  Successful MS/peer initiated deactivations: 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 | APN |
|-----------------------|----------|--------------------|--------------|-----|
| 33344444444535 | 34444535 | 100.105.24.1 | 22.0.111.111 | |
| wireless1.juniper.net | | | | |
| 66644444449456 | 64494456 | 100.105.36.3 | 88.2.111.111 | |
| wireless1.juniper.net | | | | |
| 99911444444489 | 91444489 | 100.105.28.14 | 99.0.111.111 | |
| wireless1.juniper.net | | | | |
| 88845544444518 | 84554518 | 100.105.28.5 | 55.0.111.111 | |


```

wireless1.juniper.net
22244444444552      2224444552  100.105.24.19      22.2.222.223
wireless1.juniper.net

user@pe1> show unified-edge ggsn-pgw subscribers extensive
Subscriber Information:
  IMSI: 33344444444535      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
                                     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: Sendbcast-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 431](#)
- [Overview on page 431](#)
- [Configuration on page 432](#)
- [Verification on page 438](#)

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 39: Components of the Broadband Gateway

| Property | Settings | Description |
|----------------------------------|--|--|
| Loopback address | lo0 unit 100 address 192.168.100.1/32 lo0 unit 111 address 192.168.111.1/32 lo0 unit 112 address 192.168.112.1/32 lo0 unit 121 address 192.168.121.1/32 lo0 unit 122 address 192.168.122.1/32 lo0 unit 200 address 192.168.200.1/32 | Interfaces used for 3GPP signaling and IP routing functions |
| Routing protocol | bgp | Indicates device is using BGP as routing protocol |
| MPLS protocol and LSP definition | mpls | Indicates device is using the MPLS protocol |
| RSVP | rsvp | Indicates device is using RSVP |
| Gi/SGi routing instance | VRF3 mif.0 | Mobile interface unit 0 (mif unit 0) is associated with Gi/SGi routing instance by placing the interface in VRF3 |
| Gn/S5 control connectivity | VRF11-Control lo0.111 | VRF for Gn/S5 interfaces for control |
| Gn/S5 data connectivity | VRF11-Data lo0.112 | VRF for Gn/S5 interfaces for data |
| Gp/S8 control connectivity | VRF12-Control lo0.121 | VRF for Gp/S8 interfaces for control |
| Gp/S8 data connectivity | VRF12-Data lo0.122 | VRF for Gp/S8 interfaces for data |
| RADIUS/charging connectivity | VRF2 lo0.200 | VRF for charging and RADIUS servers |

Configuration

- [Configuring the Chassis on page 433](#)
- [Configuring the MPLS/BGP VPN on page 434](#)
- [Enabling the Routing Instances for the VPN on page 435](#)

- [Configuring GTP Interfaces on page 436](#)
- [Configuring the Source Interface for RADIUS and Charging Servers on page 437](#)
- [Enabling the APN Configuration on page 437](#)

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: Sendbcast-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 440](#)
- [Overview on page 440](#)
- [Configuration on page 440](#)
- [Verification on page 443](#)

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 440](#)
- [Configuring NAT Pools and NAT Rules on page 441](#)
- [Configuring Service Sets on page 442](#)

Configuring the Chassis

CLI Quick Configuration To quickly configure this example, copy the following commands and paste them into the router terminal window:


```
[edit]
load merge /etc/config/mobility-defaults.conf
set chassis fpc 1 pic 0 apply-groups mobility
set chassis fpc 1 pic 1 adaptive-services service-package extension-provider control-cores
1
set chassis fpc 1 pic 1 adaptive-services service-package extension-provider data-cores 7
set chassis fpc 1 pic 1 adaptive-services service-package extension-provider
object-cache-size 14336
set chassis fpc 1 pic 1 adaptive-services service-package extension-provider policy-db-size
256
set chassis fpc 1 pic 1 adaptive-services service-package extension-provider package
jservices-nat
set chassis fpc 1 pic 1 adaptive-services service-package extension-provider package
jservices-alg
set chassis fpc 1 pic 1 adaptive-services service-package syslog daemon any
set chassis fpc 1 pic 1 adaptive-services service-package syslog kernel any
```

Step-by-Step Procedure

To configure the chassis:

1. Load and merge the default configuration file for the **mobility** group.

```
[edit]
user@pe1# load merge /etc/config/mobility-defaults.conf
```

2. Configure the **mobility** group on the session DPC.

```
[edit]
user@pe1# set chassis fpc 1 pic 0 apply-groups mobility
```

3. Configure the Multiservices DPC for NAT services. Specify the **jservices-nat** and **jservices-alg** packages.

```
[edit]
user@pe1# set chassis fpc 1 pic 1 adaptive-services service-package
extension-provider control-cores 1
user@pe1# set chassis fpc 1 pic 1 adaptive-services service-package
extension-provider data-cores 7
user@pe1# set chassis fpc 1 pic 1 adaptive-services service-package
extension-provider object-cache-size 14336
user@pe1# set chassis fpc 1 pic 1 adaptive-services service-package
extension-provider policy-db-size 256
user@pe1# set chassis fpc 1 pic 1 adaptive-services service-package
extension-provider package jservices-nat
user@pe1# set chassis fpc 1 pic 1 adaptive-services service-package
extension-provider package jservices-alg
```

Configuring NAT Pools and NAT Rules

CLI Quick Configuration

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]
set services nat pool pool_nat44 address-range low 19.19.19.1 high 19.19.19.32
set services nat pool pool_nat44 port automatic
set services nat rule rule_nat44 match-direction input
set services nat rule rule_nat44 term t1 from source-address 30.30.0.0/16
set services nat rule rule_nat44 term t1 then translated source-pool pool_nat44
```

```
set services nat rule rule_nat44 term t1 then translated translation-type napt-44
```

**Step-by-Step
Procedure**

To configure NAT pools and NAT rules:

1. Configure the NAT pool address as an address range.

```
[edit]  
user@pe1# set services nat pool pool_nat44 address-range low 19.19.19.1 high  
19.19.19.32
```
2. Specify that the NAT pool port is a router-assigned port.

```
[edit]  
user@pe1# set services nat pool pool_nat44 port automatic
```
3. Configure the NAT rule to match on input.

```
[edit]  
user@pe1# set services nat rule rule_nat44 match-direction input
```
4. Specify the input condition for the NAT term.

```
[edit]  
user@pe1# set services nat rule rule_nat44 term t1 from source-address 30.30.0.0/16
```
5. Specify the input actions for the NAT term.

```
[edit]  
user@pe1# set services nat rule rule_nat44 term t1 then translated source-pool  
pool_eif  
user@pe1# set services nat rule rule_nat44 term t1 then translated translation-type  
napt-44
```

Configuring Service Sets

**CLI Quick
Configuration**

To quickly configure this example, copy the following commands and paste them into the router terminal window:

```
[edit]  
set interfaces ms-1/1/0 unit 0 family inet  
set services service-set set_0 nat-rules rule_nat44  
set services service-set set_0 interface-service service-interface ms-1/1/0  
set interfaces mif unit 0 family inet service input service-set set_0  
set interfaces mif unit 0 family inet service output service-set set_0
```

**Step-by-Step
Procedure**

To configure service sets:

1. Configure the service interface associated with the service set.

```
[edit]  
user@pe1# set interfaces ms-1/1/0 unit 0 family inet
```
2. Configure the service set.

```
[edit]  
user@pe1# set services service-set set_0
```
3. Specify the NAT rules.

```
[edit]
```

```
user@pe1# set services service-set set_0 nat-rules rule_nat44
```

4. Specify the service interface.

```
[edit]
```

```
user@pe1# set services service-set set_0 interface-service service-interface ms-1/1/0
```

5. Associate the service set with the mobile interface.

```
[edit]
```

```
user@pe1# set interfaces mif unit 0 family inet service input service-set set_0
```

```
user@pe1# set interfaces mif unit 0 family inet service output service-set set_0
```

Verification

Verifying the NAT Pool Information

Purpose Verify information about NAT pools.

Action user@pe1> show services nat pool detail

```
Interface: ms-1/1/0, Service set: set_0
```

```
NAT pool: pool_nat44, Translation type: napt-44
```

```
Address range: 19.19.19.1-19.19.19.32
```

```
Address range: 2.2.2.2-2.2.2.2
```

```
Port range: 512-65535, Ports in use: 0, Out of port errors: 0, Max ports used: 0
```


PART 11

Complete Configuration Statement Hierarchy and Summary of Statements

- [Configuration Statement Hierarchy on page 447](#)
- [AAA on the Broadband Gateway on page 469](#)
- [Address Assignment and DHCP Configuration Statements on page 501](#)
- [Anchor Packet Forwarding Engine Redundancy and Aggregated Multiservices High Availability Configuration Statements on page 529](#)
- [APN Configuration Statements on page 553](#)
- [Charging Configuration Statements on page 619](#)
- [Class of Service \(CoS\) Configuration Statements on page 693](#)
- [Exception Handling Configuration Statements on page 731](#)
- [Gateway Maintenance Mode Configuration Statement on page 749](#)
- [GTP Configuration Statements on page 751](#)
- [Service Applications Configuration Statements on page 771](#)
- [System Architecture and Gateway Traceoptions Configuration Statements on page 779](#)

Configuration Statement Hierarchy

- [\[edit access\] Hierarchy Level on page 447](#)
- [\[edit access address-assignment\] Hierarchy Level on page 448](#)
- [\[edit class-of-service\] Hierarchy Level on page 449](#)
- [\[edit interfaces ams\] Hierarchy Level on page 449](#)
- [\[edit interfaces apfe\] Hierarchy Level on page 450](#)
- [\[edit interfaces mif\] Hierarchy Level on page 450](#)
- [\[edit routing-instance system\] Hierarchy Level on page 451](#)
- [\[edit services ip-reassembly\] Hierarchy Level on page 452](#)
- [\[edit services service-set\] Hierarchy Level on page 452](#)
- [\[edit unified-edge\] Hierarchy Level on page 452](#)
- [\[edit unified-edge aaa\] Hierarchy Level on page 453](#)
- [\[edit unified-edge cos-cac\] Hierarchy Level on page 454](#)
- [\[edit unified-edge gateways\] Hierarchy Level on page 456](#)
- [\[edit unified-edge local-policies\] Hierarchy Level on page 465](#)
- [\[edit unified-edge mobile-options\] Hierarchy Level on page 466](#)
- [\[edit unified-edge resource-management\] Hierarchy Level on page 466](#)

[\[edit access\] 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 {
    family family;
}
}
```

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 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);
            }
        }
        service-interface interface-name.unit-number;
    }
}
```

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 453](#)
- [\[edit unified-edge cos-cac\] Hierarchy Level on page 454](#)
- [\[edit unified-edge gateways\] Hierarchy Level on page 456](#)
- [\[edit unified-edge local-policies\] Hierarchy Level on page 465](#)
- [\[edit unified-edge mobile-options\] Hierarchy Level on page 466](#)
- [\[edit unified-edge resource-management\] Hierarchy Level on page 466](#)

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];
          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];
    }
  }
}
}
}
}
}

```

- Related Documentation**
- [\[edit unified-edge\] Hierarchy Level on page 452](#)
 - [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](#)

```

unified-edge {
  gateways {
    ggsn-pgw gateway-name {
      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;
  }
}
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;
  visited-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;
}
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-plmn-identifier;
            rat-type;
            record-sequence-number;
            served-imeisv;
            served-msisdn;
            served-pdppdn-address;
            serving-node-plmn-identifier;
            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;
  reconnect-time duration;
  source-interface interface-name [ipv4-address address];
  t3-response response-interval;
  transport-protocol (tcp | udp);
  version (v0 | v1 | v2);
  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);
  }
}
local-persistent-storage-options {
  cdrs-per-file value;
  disable-replication;
  disk-space-policy {
    watermark-level-1 (notification-level (syslog | snmp-alarm | both))
      (percentage value);
    watermark-level-2 (notification-level (syslog | snmp-alarm | both))
      (percentage value);
    watermark-level-3 (notification-level (syslog | snmp-alarm | both))
      (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;
                peer charging-gateway-peer-name;
                peer charging-gateway-peer-name;
            }
            persistent-storage-order {
                local-storage;
            }
            switch-back-time seconds;
        }
    }
    service-mode maintenance;
}
trigger-profiles profile-name {
    description string;
    exclude {
        ms-timezone-change;
        plmn-change;
        qos-change;
        rat-change;
        user-location-change;
    }
    offline {
        container-limit value;
        sgsn-sgw-change-limit value;
        time-limit value;
        volume-limit {
            value;
            direction (both | uplink);
        }
    }
    tariff-time-list {
        tariff-time;
    }
}
}
gtp {
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    n3-requests requests;

```

```

path-management (enable | disable);
t3-response response-interval;
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 [ip-address];
    n3-requests requests;
    path-management (enable | disable);
    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 [ip-address];
    n3-requests requests;
    path-management (enable | disable);
    t3-response response-interval;
}
gn {
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    interface interface-name v4-address [ip-address];
    n3-requests requests;
    path-management (enable | disable);
    t3-response response-interval;
    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 [ip-address];
        n3-requests requests;
        path-management (enable | disable);
        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 [ip-address];
        n3-requests requests;
        path-management (enable | disable);
        t3-response response-interval;
    }
}
gp {
    echo-interval interval;
    echo-n3-requests requests;

```

```
echo-t3-response response-interval;
interface interface-name v4-address [ip-address];
n3-requests requests;
path-management (enable | disable);
t3-response response-interval;
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 [ip-address];
    n3-requests requests;
    path-management (enable | disable);
    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 [ip-address];
    n3-requests requests;
    path-management (enable | disable);
    t3-response response-interval;
}
}
s5 {
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    interface interface-name v4-address [ip-address];
    n3-requests requests;
    path-management (enable | disable);
    t3-response response-interval;
    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 [ip-address];
        n3-requests requests;
        path-management (enable | disable);
        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 [ip-address];
        n3-requests requests;
        path-management (enable | disable);
        t3-response response-interval;
    }
}
```

```

}
s8 {
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    interface interface-name v4-address [ip-address];
    n3-requests requests;
    path-management (enable | disable);
    t3-response response-interval;
    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 [ip-address];
        n3-requests requests;
        path-management (enable | disable);
        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 [ip-address];
        n3-requests requests;
        path-management (enable | disable);
        t3-response response-interval;
    }
}
peer-groups peer-groups name {
    echo-interval interval;
    echo-n3-requests requests;
    echo-t3-response response-interval;
    n3-requests requests;
    path-management (enable | disable);
    peer (ip-address | ip-prefix);
    routing-instance routing-identifier;
    t3-response response-interval;
    control {
        sequence-number-length 16-bits;
    }
}
traceoptions {
    file filename <files number> <size size> ;
}
flag flag (config | debug | decode | encode | events | packet-io | peer | tracker |
    warning | all) ;
    level (error | info | notice | verbose | warning | all) ;
}
}
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-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**
- [\[edit unified-edge\] Hierarchy Level on page 452](#)
 - [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 452](#)
 - [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 452](#)
 - [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 452](#)
 - [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 108](#)

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 108](#)
- [radius on page 490](#)

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 108 • servers on page 494 |

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 108 • servers on page 494 |

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 | 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 108• servers on page 494 |

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 | 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 108• network-elements on page 486 |

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 108• servers on page 494 |

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 108](#)
- [radius on page 490](#)

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 108](#)
- [radius on page 490](#)

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 108](#)
- [servers on page 494](#)

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 108• servers on page 494 |

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 108• servers on page 494 |

exclude

```
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];
    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 attributes]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

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**—Excludes the RADIUS attribute 45, Acct-Authentic.
- **accounting-delay-time**—Excludes the RADIUS attribute 41, Acct-Delay-Time.
- **accounting-terminate-cause**—Excludes the RADIUS attribute 49, Acct-Terminate-Cause.
- **all-3gpp**—Excludes all 3GPP attributes.

- **called-station-id**—Excludes the RADIUS attribute 30, Called-Station-ID.
- **calling-station-id**—Excludes the RADIUS attribute 31, Calling-Station-ID.
- **event-timestamp**—Excludes the RADIUS attribute 55, Event-Timestamp.
- **imeisv**—Set this configuration to exclude the imeisv attribute from the access-request or accounting-start request sent to the RADIUS server.
- **imsi**—Set this configuration to exclude the imsi attribute from the requests sent to the RADIUS server.
- **imsi-mcc-mnc**—Excludes RADIUS attribute 3GPP VSA 26-8, 3GPP-IMSI-MCC-MNC.
- **input-filter**—Ignore input-filter or ingress-policy-name (VSA 26-10).
- **input-gigapackets**—Excludes the RADIUS attribute 26-42, Acct-Input-Gigapackets.
- **input-gigawords**—Excludes the RADIUS attribute 52, Acct-Input-Gigawords.
- **nas-identifier**—Excludes the RADIUS attribute 32, NAS-identifier.
- **nas-ip-address**—Excludes the RADIUS attribute, NAS-IP-address.
- **nas-port**—Excludes the RADIUS attribute 61, NAS-Port.
- **nas-port-id**—Excludes the RADIUS attribute 61, NAS-Port-Id.
- **nas-port-type**—Excludes the RADIUS attribute 61, NAS-Port-Type.
- **output-filter**—Ignore output-filter or egress-policy-name (VSA 26-11).
- **output-gigapackets**—Excludes the RADIUS attribute 26-43, Acct-Output-Gigapackets.
- **output-gigawords**—Excludes the RADIUS attribute 53, Acct-Output-Gigawords.
- **sgsn-mcc-mnc**—Set this configuration to exclude the sgsn-mcc-mnc attribute from the requests sent to the RADIUS server.
- **user-location-info**—Excludes RADIUS attribute 3GPP VSA 26-22, 3GPP-USER-LOCATION-INFO.

| | |
|---------------------------|--|
| Required Privilege | access—To view this statement in the configuration. |
| Level | 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 108• attributes on page 476 |
|------------------------------|---|

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 108 • attributes on page 476 |

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 108 • network-elements on page 486 |

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 | <ul style="list-style-type: none"> • Overview of AAA on the Broadband Gateway on page 108 • aaa on page 470 |

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 108• accounting on page 472 |

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 108• accounting on page 472 |

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 108 • radius on page 488 |

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 108• radius on page 488 |

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 108 • radius on page 490 |

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 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 108](#)

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

- [Overview of AAA on the Broadband Gateway on page 108](#)
- [aaa on page 470](#)

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 108• servers on page 494 |

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 108• servers on page 494 |

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 108 |

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 108• accounting on page 472 |

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 108](#)
- [radius on page 488](#)

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 108• servers on page 494 |

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 108• accounting on page 472 |

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 108• accounting on page 472 |

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 108• servers on page 494 |

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 108 • radius on page 488 |

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 108• aaa on page 470 |

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 | access—To view this statement in the configuration. |
| Level | 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 108• accounting on page 472 |
|------------------------------|---|

CHAPTER 19

Address Assignment and DHCP Configuration Statements

- [Address Assignment Configuration Statements on page 502](#)
- [DHCP Configuration Statements on page 513](#)

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 395](#)

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 507 |

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 556 • mobile-pools on page 507 |

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 508• range (Mobile Pools) on page 511 |

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 507](#)

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> 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.</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 502• mobile-pools on page 507 |

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 502](#)

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 511 |


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 507 |

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, another notification is sent to signal that the pool usage threshold 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 507 |

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 508 |

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 332• Deleting a Mobile Address Pool on page 334• mobile-pools on page 507 |

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 167 • dhcp-proxy-client on page 516 |

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 167• dhcp-proxy-client on page 516 |

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 167 • dhcp-proxy-client on page 516 |

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 167](#)
- [services on page 525](#)

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 167](#)
- [dhcp-proxy-client on page 516](#)

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 167• dhcp-proxy-client on page 516 |

dhcipv6-profiles

| | |
|---------------------------------|--|
| Syntax | <pre>dhcipv6-profiles <i>profile-name</i> { bind-interface <i>interface-name</i> [ip-address]; dead-server-retry-interval <i>n seconds</i>; dead-server-successive-retry-attempt <i>number-of-attempts</i>; dhcp-server-selection-algorithm (highest-priority-server round-robin); 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 { ipv6-address <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 167 • dhcp-proxy-client on page 516 |

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 167• dhcp-proxy-client on page 516 |

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 167• dhcp-proxy-client on page 516 |

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 167 • dhcp-proxy-client on page 516 |

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 167• dhcp-proxy-client on page 516 |

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 167 • dhcp-proxy-client on page 516 |

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 | IPv4—IPv4 address for the server. 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">• DHCP Overview on page 167• dhcp-proxy-client on page 516 |

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 167](#)
- [system on page 526](#)

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 167](#)

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 167• dhcp-proxy-client on page 516 |

CHAPTER 20

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 | [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> system] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>Specify the interfaces used for anchoring 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 550 |


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] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| 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 | <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 550 |

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 54 • Configuring Interface DPCs or MPCs for User Mobility Traffic on page 42 • Example: Configuring Broadband Gateway Redundancy on page 58 • interfaces (Aggregated Packet Forwarding Engine) on page 540 |

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 | apfe-group-set —Name of the apfe group set. Range: Up to 32 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">• anchoring-options (Aggregated Packet Forwarding Engine) on page 531• Configuring Interface Redundancy on page 54• Example: Configuring Broadband Gateway Redundancy on page 58 |

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 52• Example: Configuring Broadband Gateway Redundancy on page 58• member-failure-options (Aggregated Multiservices) on page 543• request interface load-balancing revert (Aggregated Multiservices) on page 834 |

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 52• Example: Configuring Broadband Gateway Redundancy on page 58• redistribute-all-traffic (Aggregated Multiservices) on page 547• request interface load-balancing revert (Aggregated Multiservices) on page 834 |

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 52• Example: Configuring Broadband Gateway Redundancy on page 58• unit (Aggregated Multiservices) on page 551 |

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 52](#)
- [Example: Configuring Broadband Gateway Redundancy on page 58](#)
- [load-balancing-options \(Aggregated Multiservices\) on page 541](#)

interface (Anchor Packet Forwarding Engine)

| | |
|---------------------------------|---|
| Syntax | <code>interface <i>interface-name</i>;</code> |
| Hierarchy Level | [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> system anchor-pfes] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>Configure the interface representing the Packet Forwarding Engine used for anchoring 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. • 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. <div style="margin-top: 10px;">  <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> </div> <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 the apfe interface apfe0, then pfe-2/0/0 cannot be directly specified here. |
| Options | <p><i>interface-name</i>—Name of the interface representing the Packet Forwarding Engine.</p> <p>Syntax: The interface must be a valid Packet Forwarding Engine interface (apfe or pfe-); for example, apfe0 or pfe-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"> • [edit unified-edge gateways] Hierarchy Level on page 456 • Configuring Interface Redundancy on page 54 • Configuring Interface DPCs or MPCs for User Mobility Traffic on page 42 • Example: Configuring Broadband Gateway Redundancy on page 58 |

interface (Multiservices PIC)

| | |
|---------------------------------|---|
| Syntax | <code>interface <i>interface-name</i>;</code> |
| Hierarchy Level | [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> system anchor-spics] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>Configure the interface representing the Multiservices PIC used for the mobile control plane in the broadband gateway. The following conditions are applicable to the Multiservices 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 Multiservices PIC must have the jservices-mobile package configured at the [edit chassis fpc slot-number pic pic-number adaptive-services service-package extension-provider] hierarchy level.• If a Multiservices 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 Multiservices PIC or aggregated Multiservices 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">• [edit unified-edge gateways] Hierarchy Level on page 456• Configuring Anchor Session DPCs and PFEs on page 47• show unified-edge ggsn-pgw system interfaces on page 842 |

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 {
    family family;
}

```

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**
- [Configuring Session DPC Redundancy on page 52](#)
 - [Example: Configuring Broadband Gateway Redundancy on page 58](#)

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 54](#)
 - [Example: Configuring Broadband Gateway Redundancy on page 58](#)

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 52](#)
- [Example: Configuring Broadband Gateway Redundancy on page 58](#)

- [interfaces \(Aggregated Multiservices\) on page 539](#)

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. |
| <div> NOTE: The preferred backup must be one of the member interfaces (<i>mams-</i>) that have already been configured at the [edit interfaces <i>interface-name</i> 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.</div> | |
| 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 52• Example: Configuring Broadband Gateway Redundancy on page 58• high-availability-options (Aggregated Multiservices) on page 536 |

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 40 on page 543 displays the behavior of the member interface after the failure of the first multiservices PIC. Table 41 on page 544 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 40: 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 41: 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 52](#)
 - [Example: Configuring Broadband Gateway Redundancy on page 58](#)
 - [load-balancing-options \(Aggregated Multiservices\) on page 541](#)
 - [request interface load-balancing revert \(Aggregated Multiservices\) on page 834](#)

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 52 • Example: Configuring Broadband Gateway Redundancy on page 58 • load-balancing-options (Aggregated Multiservices) on page 541 |

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. |
| | <div> 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.</div> |
| | <p>To configure multiple primary FPCs, include the anchoring-device-name statement multiple times.</p> |
| Options | <i>anchoring-device-name</i> —Name of the FPC. |
| | <div> NOTE: The interface must be a valid interface (<i>fpc-</i>) that is defined in the broadband gateway interface hierarchy.</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">• anchoring-options (Aggregated Packet Forwarding Engine) on page 531• Configuring Interface Redundancy on page 54• Configuring Interface DPCs or MPCs for User Mobility Traffic on page 42• Example: Configuring Broadband Gateway Redundancy on page 58 |

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 52• Example: Configuring Broadband Gateway Redundancy on page 58• member-failure-options (Aggregated Multiservices) on page 543 |

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 52• drop-member-traffic (Aggregated Multiservices) on page 533• Example: Configuring Broadband Gateway Redundancy on page 58• request interface load-balancing revert (Aggregated Multiservices) on page 834 |

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 | 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">• anchoring-options (Aggregated Packet Forwarding Engine) on page 531• Configuring Interface Redundancy on page 54• Example: Configuring Broadband Gateway Redundancy on page 58 |
|------------------------------|--|

system

| | |
|---------------------------------|--|
| Syntax | <pre>system { anchor-pfes { interface <i>interface-name</i>; } anchor-spics { interface <i>interface-name</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>Specify the interfaces used for anchoring and the mobile control plane 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">• [edit unified-edge gateways] Hierarchy Level on page 456 |

unit (Aggregated Multiservices)

Syntax `unit interface-unit-number {
 family family;
}`

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 52](#)
- [Example: Configuring Broadband Gateway Redundancy on page 58](#)
- [interfaces \(Aggregated Multiservices\) on page 539](#)

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 531• Configuring Interface Redundancy on page 54• Example: Configuring Broadband Gateway Redundancy on page 58 |

CHAPTER 21

APN Configuration Statements

- [APN Services Configuration Statements on page 553](#)
- [Service Selection Profiles Configuration Statements on page 604](#)

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 556• Enabling Address Assignment by the RADIUS Server on page 151• Configuring Address Assignment on a Broadband Gateway APN on page 89 |

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 151• dhcp-proxy-client (APN Address Assignment) on page 569• local (APN Address Assignment) on page 582 |

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 563 • Configuring General APN Parameters on the Broadband Gateway on page 83 • Example: Configuring Broadband Gateway APNs on page 100 |

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 502](#)
- [apns on page 563](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 89](#)
- [Example: Configuring Broadband Gateway APNs on page 100](#)

allow-static-ip-address (APN Address Assignment)

Syntax `allow-static-ip-address {
 no-address-verify;
}`

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name* apn-services apns *name* address-assignment]

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 allowed by the broadband gateway. The gateway obtains the IP address of the user equipment from the Create Session Request message.

The remaining statement is explained separately.

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

- [address-assignment \(APN\) on page 556](#)
- [Configuring Address Assignment on a Broadband Gateway APN on page 89](#)

anonymous-user (APN)

Syntax `anonymous-user {
 password password;
 (use-apnname | use-imsi | use-msisdn | user-name username);
 }`

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 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.

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.

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.



NOTE: The information about the AAA server is obtained from the AAA profile that you specify for the APN.

Options `password password`—Password for user authentication.

Range: Up to 32 characters

`use-apnname | use-imsi | use-msisdn | user-name username`—Choose the type of username to be used for anonymous users in the APN.

- **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.
- **username**—Default username to be used for authentication.

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 563](#)
 - [Configuring Anonymous Users on a Broadband Gateway APN on page 88](#)

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 | <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 563 • Configuring General APN Parameters on the Broadband Gateway on page 83 |

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;
                }
            }
        }
        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;
            visited-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;
}
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 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.

The APN selection function determines which APN and service types a Mobile Station (MS) or user equipment (UE) device should use.

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 456• Configuring APNs on the MobileNext Broadband Gateway Overview on page 79• Example: Configuring Broadband Gateway APNs on page 100 |

apn-type

| | |
|---------------------------------|---|
| Syntax | apn-type (real virtual virtual-pre-authenticate); |
| 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>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 | 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 563• Configuring General APN Parameters on the Broadband Gateway on page 83 |

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;
            }
        }
        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;
            visited-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;
}
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 <i>gateway-name</i> apn-services] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>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.</p> <p>The remaining statements are explained separately.</p> |
| 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**
- [apn-services on page 560](#)
 - [Configuring APNs on the MobileNext Broadband Gateway Overview on page 79](#)
 - [Configuring General APN Parameters on the Broadband Gateway on page 83](#)
 - [Example: Configuring Broadband Gateway APNs on page 100](#)

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 563 • Configuring General APN Parameters on the Broadband Gateway on page 83 |

charging (APN)

| | |
|----------------------------|--|
| Syntax | <pre>charging { default-profile default-profile; home-profile home-profile; profile-selection-order [profile-selection-method]; roamer-profile roamer-profile; visited-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 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 563 • Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 93 • charging-profiles on page 628 |

default-profile (APN)

| | |
|----------------------------|---|
| 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] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | Specify the default charging profile for the access point name (APN). 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 for the APN, then the default charging 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 it 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 **default-profile** is also not configured, then the subscriber session is created without charging enabled.

| | |
|---------------------------------|---|
| Options | <i>default-profile</i> —Name of the default charging 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"> • Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 93 • charging (APN) on page 566 • charging-profiles on page 628 |


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 563• Configuring General APN Parameters on the Broadband Gateway on page 83 |


dhcp-proxy-client (APN Address Assignment)

| | |
|---------------------------------|--|
| Syntax | dhcp-proxy-client { 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 | <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 | <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"> • address-assignment (APN) on page 556 • Configuring Address Assignment on a Broadband Gateway APN on page 89 • Example: Configuring Broadband Gateway APNs on page 100 |

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><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> | |
| <hr/> <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 556• Configuring DHCP Under APN on page 169• Configuring Address Assignment on a Broadband Gateway APN on page 89 |


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 556 • Configuring DHCP Under APN on page 169 • Configuring Address Assignment on a Broadband Gateway APN on page 89 |

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 563• Configuring General APN Parameters on the Broadband Gateway on page 83 |

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 89 • inet-pool (APN Address Assignment) on page 579 |

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 89• inet6-pool (APN Address Assignment) on page 580 |

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>  <p>NOTE: You can specify either a mobile pool group or a mobile pool, 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>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 89 • inet-pool (APN Address Assignment) on page 579 • inet6-pool (APN Address Assignment) on page 580 • mobile-pool-groups on page 506 |

home-profile (APN)

| | |
|----------------------------|---|
| 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] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | Specify the home charging profile for the access point name (APN) that should be used to charge home subscribers. If the profile-selection-order configuration indicates static , then this profile is used for members of the broadband gateway's home public land mobile network (HPLMN). |



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 match the corresponding values configured for the HPLMN and if the subscriber's Routing Area Identity (RAI) matches the corresponding RAI configured for the HPLMN, 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 **default-profile** is also not configured, then the subscriber session is created without charging enabled.

| | |
|---------------------------------|---|
| Options | <i>home-profile</i> —Name of the home charging 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">• Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 93• charging (APN) on page 566• charging-profiles on page 628 |


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 563• Configuring General APN Parameters on the Broadband Gateway on page 83• idle-timeout-direction (APN) on page 578 |


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 563• Configuring General APN Parameters on the Broadband Gateway on page 83• idle-timeout (APN) on page 577 |

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 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 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 | <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"> • address-assignment (APN) on page 556 • Configuring Address Assignment on a Broadband Gateway APN on page 89 |


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><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 556• Configuring Address Assignment on a Broadband Gateway APN on page 89 |


inter-mobile-traffic (APN)

| | |
|---------------------------------|---|
| Syntax | inter-mobile-traffic { (deny redirect <i>redirect</i>); } |
| 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 563 • Configuring General APN Parameters on the Broadband Gateway on page 83 |

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> NOTE: An APN can have a mobile pool or a mobile pool group configured, but not both.</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 556• Configuring AAA-Assigned Addresses to Override Locally or DHCP-Assigned Addresses on page 151 |

local-policy-profile (APN)

| | |
|---------------------------------|---|
| Syntax | <code>local-policy-profile <i>local-policy-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 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>  <p>NOTE: The local-policy-profile must already be configured at the <code>[edit unified-edge]</code> hierarchy level.</p> </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 563 • Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 93 • local-policy-profile (MobileNext Broadband Gateway) on page 713 |



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 169• Configuring Address Assignment on a Broadband Gateway APN on page 89• dhcpv4-proxy-client-profile (APN Address Assignment) on page 570• dhcpv6-proxy-client-profile (APN Address Assignment) on page 571 |

maximum-bearers (APN)

| | |
|---------------------------------|---|
| Syntax | maximum-bearers <i>maximum-bearers</i> ; |
| 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 563 • Configuring General APN Parameters on the Broadband Gateway on page 83 • Configuring the Maximum Number of Bearers on page 254 • maximum-bearers (MobileNext Broadband Gateway) on page 715 |

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 | <p>Configure the mobile interface for the access point name (APN).</p> <p>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.</p> <div> NOTE: The configuration of a mobile interface is mandatory.</div> |
| Options | <p><code>mobile-interface</code>—Mobile interface name.</p> <div> NOTE: The interface must be defined as a mobile interface (mif-) in the broadband gateway interface hierarchy.</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">• apns on page 563• Configuring General APN Parameters on the Broadband Gateway on page 83• Configuring Mobile Interfaces for APNs on page 94• interfaces (Mobile Interface) on page 785 |

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 563 • Configuring General APN Parameters on the Broadband Gateway on page 83 |


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 | 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">• allow-static-ip-address (APN Address Assignment) on page 557• Configuring Address Assignment on a Broadband Gateway APN on page 89 |

p-cscf (APN)

| | |
|---------------------------------|---|
| Syntax | <code>p-cscf { [<i>address</i>]; }</code> |
| 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 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><i>address</i>—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 563 • Configuring General APN Parameters on the Broadband Gateway on page 83 |


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> NOTE: You can specify either a mobile pool or a mobile pool group, 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>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 89• inet-pool (APN Address Assignment) on page 579• inet6-pool (APN Address Assignment) on page 580• mobile-pools on page 507 |


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 169 • Configuring Address Assignment on a Broadband Gateway APN on page 89 • dhcpv4-proxy-client-profile (APN Address Assignment) on page 570 • dhcpv6-proxy-client-profile (APN Address Assignment) on page 571 |

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> 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.</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 169• Configuring Address Assignment on a Broadband Gateway APN on page 89• dhcpv4-proxy-client-profile (APN Address Assignment) on page 570• dhcpv6-proxy-client-profile (APN Address Assignment) on page 571• mobile-pools on page 507 |

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 style="margin-top: 20px;">  <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 93 • charging (APN) on page 566 |

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 42 on page 594](#) displays the valid restriction values that you can configure.

Table 42: 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 563 • Configuring the Restriction Value on a Broadband Gateway APN on page 87 |

roamer-profile (APN)

| | |
|----------------------------|--|
| 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] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | Configure the charging profile for the access point name (APN) that should be used to charge roaming subscribers. If the profile-selection-order configuration indicates static , then this profile is used for members of the broadband gateway's roamer public land mobile network (PLMN). |



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 match the corresponding values configured for the home PLMN, but the subscriber's Routing Area Identity (RAI) does not match the corresponding RAI configured for the home 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 **default-profile** is also not configured, then the subscriber session is created without charging enabled.

| | |
|---------------------------------|---|
| Options | <i>roamer-profile</i> —Name of the roamer charging 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"> • Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 93 • charging (APN) on page 566 • charging-profiles on page 628 |

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 169• Configuring Address Assignment on a Broadband Gateway APN on page 89• dhcpv4-proxy-client-profile (APN Address Assignment) on page 570• dhcpv6-proxy-client-profile (APN Address Assignment) on page 571 |

selection-mode (APN)

| | |
|----------------------------|---|
| Syntax | selection-mode { (from-ms from-sgsn no-subscribed); } |
| 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 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 43 on page 597 displays the selection mode IE values and their descriptions.</p> <p>The following selection mode options can be configured for the APN:</p> <ul style="list-style-type: none"> • 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 43: 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 563](#)
- [Configuring General APN Parameters on the Broadband Gateway on page 83](#)

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 563](#)
- [Configuring the Mobile Interface of an Access Point Name on page 323](#)
- [Deleting an Access Point Name on page 325](#)
- [Example: Changing Access Point Name Values on page 335](#)
- [Modifying an Access Point Name on page 322](#)

service-selection-profile (APN)

| | |
|---|--|
| Syntax | <code>service-selection-profile <i>service-selection-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 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. |
| <div>  <p>NOTE: The service selection profile must be already configured on the broadband gateway.</p> </div> | |
| Options | <code>service-selection-profile</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 563 • Configuring APN Service Selection on a Broadband Gateway on page 97 • service-selection-profiles on page 615 |

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 563• Configuring General APN Parameters on the Broadband Gateway on page 83 |

verify-source-address (APN)

| | |
|---------------------------------|--|
| Syntax | verify-source-address { disable; } |
| 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 563 • Configuring General APN Parameters on the Broadband Gateway on page 83 |

visited-profile (APN)

| | |
|----------------------------|--|
| Syntax | <code>visited-profile <i>visited-profile</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 | Specify the charging profile for the access point name (APN) that should be used to charge visiting subscribers. If the profile-selection-order configuration indicates static , then this profile is used for subscribers who are not members of the broadband gateway's home public land mobile network (HPLMN), but are visiting. |



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 match the corresponding values configured for the home PLMN, then the subscriber is deemed a visitor and the **visited-profile** is applied. If the **visited-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 without charging enabled.

| | |
|---------------------------------|---|
| Options | <i>visited-profile</i> —Name of the visited charging 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">• Configuring Charging and Local Policy Profiles on a Broadband Gateway APN on page 93• charging (APN) on page 566• charging-profiles on page 628 |

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 563 • Configuring General APN Parameters on the Broadband Gateway on page 83 |

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 97• then (Service Selection Profiles) on page 617 |

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 97• from (Service Selection Profiles) on page 606 |

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 interface—To view this statement in the configuration.
Level interface-control—To add this statement to the configuration.

Related • [Configuring APN Service Selection on a Broadband Gateway on page 97](#)
Documentation • [term \(Service Selection Profiles\) on page 616](#)

imei (Service Selection Profiles)

| | |
|--------------------------|---|
| Syntax | imei <i>imei</i> ; |
| Hierarchy Level | [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> service-selection-profiles <i>profile 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 97 • from (Service Selection Profiles) on page 606 |


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 97• from (Service Selection Profiles) on page 606 |

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 97 • from (Service Selection Profiles) on page 606 |

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 97• from (Service Selection Profiles) on page 606 |


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>ipv4—Match PDNs supporting only IPv4.</p> <p>ipv4v6—Match PDNs supporting both IPv4 and IPv6.</p> <p>ipv6—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 97 • from (Service Selection Profiles) on page 606 |

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 | peer —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 97 • from (Service Selection Profiles) on page 606 |

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 97• from (Service Selection Profiles) on page 606 |

profile (Service Selection Profiles)

```
Syntax  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* service-selection-profiles]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description 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.

The remaining statements are explained separately.

Options *name*—Name of the service selection profile.
Syntax: 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

- [Configuring APN Service Selection on a Broadband Gateway on page 97](#)
- [service-selection-profiles on page 615](#)

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 97• then (Service Selection Profiles) on page 617 |

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 97](#)
- [Example: Configuring Broadband Gateway APNs on page 100](#)

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 97• profile (Service Selection Profiles) on page 613 |

then (Service Selection Profiles)


| | |
|---------------------------------|--|
| Syntax | <pre> then { apn-name apn-name; redirect-peer redirect-peer; } </pre> |
| Hierarchy Level | [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> service-selection-profiles profile <i>name</i> term <i>name</i>] |
| 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. |
| | <div>  <p>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.</p> </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"> • Configuring APN Service Selection on a Broadband Gateway on page 97 • term (Service Selection Profiles) on page 616 |

Charging Configuration Statements

cdr-aggregation-limit

| | |
|---------------------------------|---|
| Syntax | <code>cdr-aggregation-limit <i>value</i>;</code> |
| Hierarchy Level | [edit unified-edge gateways ggsn-pgw <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. |
| Description | <p>Configure the cdr-aggregation-limit attribute, which represents the maximum number of CDRs that can be added to a DRT message before it is transmitted.</p> <p>A Data Record Transfer (DRT) message containing the CDRs is transmitted from the CDF to the 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.</p> |
| Options | <p><i>value</i>—Number of CDRs that can be added to a DRT message.</p> <p>Range: 1 through 16</p> <p>Default: 5</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 627 • Configuring Transport Profiles on page 226 • Configuring Charging on page 219 |

cdr-profile

| | |
|---------------------------------|---|
| Syntax | <code>cdr-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> |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>Associate a 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 to which it is associated is under active maintenance mode. Use the following command to bring the charging profile under maintenance mode:</p> <p><code>set unified-edge gateways ggsn-pgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i> service-mode maintenance</code></p> <div><p>TIP: If the profile has not been defined previously, use the following command to define a new cdr profile:</p><p><code>set unified-edge gateways ggsn-pgw <i>gateway-name</i> charging cdr-profiles <i>profile-name</i></code></p></div> |
| Options | <i>profile-name</i> —Name of the CDR 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 628• Configuring Charging Profiles on page 231• Configuring Charging on page 219• Charging Profiles on page 217 |

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-plmn-identifier;
 rat-type;
 record-sequence-number;
 served-imeisv;
 served-msisdn;
 served-pdppdn-address;
 serving-node-plmn-identifier;
 start-time;
 stop-time;
 user-location-information;
 }
 }`

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name* charging]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

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 a P-GW is 16.

The remaining statements are explained separately.

Options *profile-name*—Name of the CDR profile.

Range: 1 through 128 bytes

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 624](#)
- [Configuring CDR Attributes on page 229](#)
- [Configuring Charging on page 219](#)

cdr-release

Syntax `cdr-release (r7 | r8 | r99);`

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name* charging transport-profiles *profile-name* offline charging-gateways]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description The encoding of the CDR is compliant with the 3GPP technical specification release version that is configured using the statement. The possible release versions are: **r7**, **r8**, or **r99**.

Options

- r7—3GPP release version, 7.
- r8—3GPP release version, 8.
- r99—3GPP release version, 99.


Default: r8

Required Privilege interface—To view this statement in the configuration.
Level interface-control—To add this statement to the configuration.

Related Documentation

- [charging-gateways on page 627](#)
- [Configuring Transport Profiles on page 226](#)
- [Configuring Charging on page 219](#)

cdrs-per-file

| | |
|---------------------------------|---|
| Syntax | <code>cdrs-per-file value;</code> |
| Hierarchy Level | [edit unified-edge gateways ggsn-pgw gateway-name charging local-persistent-storage-options] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>The files containing the CDRs are copied from a temporary location on the RE disk to a final location within the same RE disk, from where these files can be SFTP transferred. However, any one of the following conditions must be met (whichever comes first):</p> <ul style="list-style-type: none"> • The number of CDRs per file reaches the configured or default limit. • The size of the file reaches the configured or default limit. • The 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> |
| | <p>Using this statement, you can configure the maximum number of CDRs that can be added to a file after which the CDR file is closed and copied to a final location within the same disk (<code>/opt/mobility/charging/ggsn/final_log</code>) from where it can be transferred via SFTP. The files thus transferred from the final location should be deleted from the local RE disk after the transfer. Only authorized users can perform this operation.</p> |
| Options | <p><i>value</i>—The maximum number of CDRs that can be added to a file after which it is closed and copied to a location within the RE disk, from where it can be SFTP transferred.</p> <p>Range: 5000 through 1,000,000</p> <p>Default: 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"> • local-persistent-storage-options on page 653 • Configuring Persistent Storage on page 222 • Configuring Charging on page 219 |

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-plmn-identifier;
                rat-type;
                record-sequence-number;
                served-imeisv;
                served-msisd;
                served-pdppdn-address;
                serving-node-plmn-identifier;
                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;
            reconnect-time duration;
            source-interface interface-name [ipv4-address address];
            t3-response response-interval;
            transport-protocol (tcp | udp);
            version (v0 | v1 | v2);
```



```

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);
}
}
local-persistent-storage-options {
  cdrs-per-file value;
  disable-replication;
  disk-space-policy {
    watermark-level-1 (notification-level (syslog | snmp-alarm | both)) (percentage value);
    watermark-level-2 (notification-level (syslog | snmp-alarm | both)) (percentage value);
    watermark-level-3 (notification-level (syslog | snmp-alarm | both)) (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;
      }
    }
  }
}

```

```
        peer charging-gateway-peer-name;  
        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;  
    }  
}
```

| | |
|---------------------------------|--|
| 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>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 | <p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p> |

- Related Documentation**
- [ggsn-pgw on page 782](#)
 - [Configuring Charging on page 219](#)
 - [Charging on page 211](#)
 - [Charging Services Overview on page 211](#)
 - [Charging Data Records on page 213](#)
 - [Charging Profiles on page 217](#)

charging-gateways

Syntax

```
charging-gateways {
  cdr-aggregation-limit value;
  cdr-release (r7 | r8 | r99);
  mtu value;
  peer-order {
    peer charging-gateway-peer-name;
    peer charging-gateway-peer-name;
    peer charging-gateway-peer-name;
  }
  persistent-storage-order {
    local-storage;
  }
  switch-back-time seconds;
}
```

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name* charging transport-profiles *profile-name* offline]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure a group of GTP Prime peers, the local RE disk, or both for CDR file storage. In addition, you can configure:

- The maximum CDRs that can be added to a DRT message.
- The maximum transmission unit of a DRT message.
- The generated CDRs to be compliant with a specific 3GPP release.
- The duration the 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.

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**
- [offline on page 658](#)
 - [Configuring Transport Profiles on page 226](#)
 - [Configuring Charging on page 219](#)

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>transport-profile profile-name</i>; <i>trigger-profile profile-name</i>; <i>service-mode maintenance</i>; }</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 | <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>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 624• Configuring Charging Profiles on page 231• Charging Profiles on page 217• Configuring Charging on page 219 |

container-limit

| | |
|---------------------------------|--|
| Syntax | <code>container-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 containers that can be added to a CDR. When the limit is reached, the CDR is closed. |
| Options | <p><i>value</i>—Maximum number of containers.</p> <p>Range: 1 through 15</p> <p>Default: 5</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 659 • Configuring Charging Trigger Events on page 227 • Configuring Charging on page 219 |

default-rating-group

| | |
|---------------------------------|---|
| Syntax | <code>default-rating-group <i>rg-num</i>;</code> |
| Hierarchy Level | [edit unified-edge gateways <i>ggsn-pgw gateway-name</i> charging charging-profiles <i>profile-name</i>] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| 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 CDR release used is <i>r7</i>, then the P-GW generates a service data container, which gets added to the CDR.</p> |
| Options | <i>rg-num</i> —The 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 628 • Configuring Charging Profiles on page 231 • Charging Profiles on page 217 • Configuring Charging on page 219 |

default-service-id

| | |
|---------------------------------|---|
| Syntax | <code>default-service-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> |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| 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 CDR release used is r7, then the P-GW generates a service data container, which gets added to the CDR.</p> |
| Options | <i>id-num</i> —The default service identifier 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 628• Configuring Charging Profiles on page 231• Charging Profiles on page 217• Configuring Charging on page 219 |

description

| | |
|---------------------------------|---|
| Syntax | <code>description <i>string</i>;</code> |
| 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 ggsn-pgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i>]</p> <p>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i>]</p> <p>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i>]</p> |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>Enter a description for the CDR profile, charging profile, transport profile, or trigger profile (which can be used to capture the purpose of the profile). For example, you may 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><i>string</i>—Description of the profile.</p> <p>Range: 255 characters or fewer</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 621 • charging-profiles on page 628 • transport-profiles on page 681 • trigger-profiles on page 684 • Configuring CDR Attributes on page 229 • Configuring Charging Profiles on page 231 • Configuring Transport Profiles on page 226 • Configuring Charging Trigger Events on page 227 |

destination-ipv4-address

| | |
|---------------------------------|---|
| Syntax | <code>destination-ipv4-address <i>address</i>;</code> |
| Hierarchy Level | [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging gtp-peer <i>peer-name</i>] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | Configure the CGF server's (GTP Prime peer's) IPv4 address, to which the CDRs are sent as GTP Prime messages from the CDF. This is a mandatory configuration. |
| Options | <i>address</i> —The 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 on page 660• Configuring GTP Prime Peers on page 221• Configuring GTP Prime for Charging on page 220 |

destination-port

| | |
|---------------------------------|--|
| Syntax | <code>destination-port <i>port-number</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>] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | Configure the TCP or UDP port on which the CGF server listens to the GTP Prime messages sent from the CDF. When there are global-level and peer-level configurations, the peer-level configuration takes precedence. |
| Options | <i>port-number</i> —The TCP or UDP port on which the CGF server listens to the GTP Prime messages sent from CDF. Range: 1 through 65,535 Default: 3386 |
| 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 651 • peer on page 660 • Configuring GTP Prime Peers on page 221 • Configuring GTP Prime for Charging on page 220 |

direction

| | |
|---------------------------------|--|
| 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] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>Configure the direction to:</p> <ul style="list-style-type: none">• both—If the configured volume-limit must include the total volume of data transmitted in both uplink and downlink directions.• uplink—If the configured volume-limit must include the volume of data transmitted in the uplink direction only. <p>When the configured 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 have impact on a previously established session. The updated configuration applies only to the new sessions.</p> |
| Default | both |
| 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 687• Configuring Charging Trigger Events on page 227• Configuring Charging on page 219 |

disable-replication

| | |
|---------------------------------|--|
| Syntax | disable-replication; |
| Hierarchy Level | [edit unified-edge gateways <i>ggsn-pgw gateway-name</i> charging local-persistent-storage-options] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>Typically, the CDRs stored on RE disk are replicated to the standby RE, as backup. However, using this statement, you can specify that the files must not be replicated to the standby RE.</p> <p>By default, replication is enabled.</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 653• Configuring Persistent Storage on page 222• Configuring Charging on page 219 |

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] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>When you use the RE disk to store CDRs, you may want to monitor and raise alerts if the disk space falls below a certain 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 | <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 653• Configuring Persistent Storage on page 222• Configuring Charging on page 219 |

down-detect-time

| | |
|---------------------------------|--|
| Syntax | <code>down-detect-time <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>] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>Configure the duration for which the CDF must wait for a response from the CGF server after the expiry of an $n3 * t3$ cycle, after which the server's status is marked Down. The CDF then proceeds to send 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 proceeds to send 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 651 • peer on page 660 • Configuring GTP Prime Peers on page 221 • Configuring GTP Prime for Charging on page 220 • Configuring Charging on page 219 |

echo-interval

| | |
|---------------------------------|--|
| Syntax | <code>echo-interval <i>duration</i>;</code> |
| Hierarchy Level | [edit unified-edge gateways <i>ggsn-pgw gateway-name</i> charging <i>gtp</i>] [edit unified-edge gateways <i>ggsn-pgw gateway-name</i> charging <i>gtp</i> peer <i>peer-name</i>] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>Configure the number of seconds that the CDF must wait before sending an echo-request message to the 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 | <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 651• peer on page 660• Configuring GTP Prime Peers on page 221• Configuring GTP Prime for Charging on page 220• Configuring Charging on page 219 |

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>] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>Enable the generation of reduced partial CDRs (RPCs). The 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.</p> |
| Default | <p>If this statement is not configured, the generation of Fully Qualified Partial CDR (FQPC) is supported.</p> <p>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.</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 621• Configuring CDR Attributes on page 229• Configuring Charging on page 219 |

exclude (Trigger Profiles)

| | |
|----------------------------|--|
| Syntax | <pre>exclude { ms-timezone-change; plmn-change; qos-change; rat-change; sgsn-sgw-change; user-location-change; }</pre> |
| Hierarchy Level | [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i> offline] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| 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 CDR.</p> <p>For example, a quality of service (QoS) change results in a container being added to the CDR. However, the container does not get added if you configure to ignore this change, using the following command:</p> <pre>set unified-edge gateways ggsn-pgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i> exclude qos-change</pre> <p>You may have configured certain IEs to be excluded from the CDR using the statements under the cdr-profiles > exclude-ie-options hierarchy. Irrespective of this configuration, some of the IEs get added to the CDR, if the corresponding triggering event is not disabled. The following table lists the triggers and the corresponding IEs.</p> |

Table 44: Triggers and corresponding IEs

| Trigger | IE |
|----------------------|------------------------------|
| ms-timezone-change | MS time zone |
| plmn-change | Serving node PLMN identifier |
| rat-change | RAT type |
| user-location-change | User location information |

- Options**
- **ms-timezone-change**—Usually, an MS time zone change results in the CDR getting updated with the charging information and the CDR getting closed. However, by configuring this statement, you can exclude charging data updates to the CDR when there is a change in the mobile station (MS) time zone.
 - **plmn-change**—Usually, a public land mobile network (PLMN) change results in the CDR getting updated with the charging information and the CDR getting closed.

However, by configuring this statement, you can exclude charging data updates to the CDR when there is a PLMN change.

- **qos-change**—Usually, a container gets added to the CDR when there is a QoS change. However, by configuring this statement, you can exclude charging data updates to the CDR when there is a QoS change.
- **rat-change**—Usually, a RAT change results in the CDR getting updated with the charging information and the CDR getting closed. However, by configuring this statement, you can exclude charging data updates to the CDR when there is a RAT change.
- **sgsn-sgw-change**—Usually, when the SGSN or SGW changes reaches the maximum configuration limit (determined by the value set for the **sgsn-sgw-change-limit** parameter), the CDR gets updated and closed. However, by configuring this statement, you can exclude charging data updates to the CDR when this limit is reached.
- **user-location-change**—Usually, a change in the user location information (such as ECGI, TAI, RAI, SAI, LAI, or CGI) results in the open containers getting closed and added to the CDR. However, by configuring this statement, you can exclude charging data updates to the CDR when there is a change in user location.

| | |
|---------------------------|---|
| 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">• offline on page 659• Configuring Charging Trigger Events on page 227• Configuring Charging on page 219 |
|------------------------------|--|

exclude-ie-options

Syntax `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-plmn-identifier;
 rat-type;
 record-sequence-number;
 served-imeisv;
 served-msisdn;
 served-pdppdn-address;
 serving-node-plmn-identifier;
 start-time;
 stop-time;
 user-location-information;
 }`

Hierarchy Level `[edit unified-edge gateways ggsn-pgw gateway-name charging cdr-profiles profile-name]`

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description The mobile operator can provision certain optional information elements (parameters) to be excluded from the 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.



CAUTION: Some of the IEs get added to the CDR irrespective of whether or not you have configured them to be excluded, if the corresponding triggering events are enabled. For the `ms-time-zone`, `serving-node-plmn-identifier`, `rat-type`, and `user-location-information` IEs, 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, they get added to the CDR.

Options

- **apn-ni**—Access point name Network Identifier (APN-NI).
APN-NI defines the external network that the user wants to connect to through gateway GPRS support node (GGSN).

- **apn-selection-mode**—This 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-subscription. The possible values for this mode are:
 - **Mobile Station**—MS-provided APN, subscription not verified.
This mode 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.
This mode 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.
This mode 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**—This mode indicates the type of charging characteristic that the GGSN or P-GW applies to the CDR. The possible selection modes are: **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 entire list, you may want to 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 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, 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**—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 gets 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 is 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 packet data network and the mobile station (MS).

This information element is applicable for CDRs that is compliant with the 3GPP R8 release specification, only.

- **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 mobile station (MS). RAT types can be eUTRAN, GERAN, WLAN, GAN, HSPA Evolution, or evolved High Rate Packet Data (eHRPD).

This IE gets 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**—Record-sequence-number is 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 ME.
- **served-msisdn**—The mobile station (MS) ISDN number (MSISDN) 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 gets 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 is compliant with the 3GPP R8 release specification, only.

- **start-time**—The 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 is compliant with the 3GPP R8 release specification, only.

- **stop-time**—The time when the user IP-CAN session is terminated for the last bearer in this session.


This information element is applicable for CDRs that is 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 excluded from the CDR too.

This IE gets 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 621 • Configuring CDR Attributes on page 229 • Configuring Charging on page 219 |

file-age

| | |
|---------------------------------|---|
| Syntax | <code>file-age value;</code> |
| Hierarchy Level | [edit unified-edge gateways ggsn-pgw gateway-name charging local-persistent-storage-options] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>The files containing the CDRs are copied from a temporary location on the RE disk to a final location within the same RE disk, from where these files can be SSH File Transfer Protocol (SFTP) transferred. However, any one of the following conditions must be met (whichever comes first):</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> <p>Using this statement, you can configure the duration, in minutes, after which the CDR file is closed and copied to a final location within the same disk (<code>/opt/mobility/charging/ggsn/final_log</code>) from where it can be transferred via SFTP. The files thus transferred from the final location should be deleted from the local RE disk after the transfer. Only authorized users can perform this operation.</p> |
| Options | <p><i>value</i>—The duration, in minutes, after which a CDR file is closed and copied to a final location within the RE disk, from where it can be SFTP transferred.</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 653• Configuring Persistent Storage on page 222• Configuring Charging on page 219 |

file-creation-policy

| | |
|---------------------------------|--|
| Syntax | file-creation-policy (shared-file unique-file); |
| Hierarchy Level | [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging local-persistent-storage-options] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | The CDRs generated for a specific transport profile from all the Service PICs can be routed to a single temporary file (shared-file configuration) or to multiple files (with each file storing CDRs generated from a single Service PIC— unique-file configuration). Configure shared-file or unique-file to meet your requirements. |
| Options | <p>shared-file—This is the default option. The 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 Service 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 (/opt/mobility/charging/ggsn/final_log).</p> <p>unique-file—The 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 Service 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 (/opt/mobility/charging/ggsn/final_log).</p> <p>Default: shared-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 653 • Configuring Persistent Storage on page 222 • Configuring Charging on page 219 |

file-format

| | |
|---------------------------------|--|
| Syntax | file-format (3gpp raw-asn); |
| Hierarchy Level | [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging local-persistent-storage-options] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | Select 3gpp to store the CDR files in a format that is compliant with the 3GPP 32297 technical specification release. Select raw-asn to store the CDR files in raw ASN1 format. |
| Options | <p>3gpp—The CDR files are stored in a format that is compliant with the 3GPP 32297 technical specification release.</p> <p>raw-asn—The CDR files are stored in raw ASN1 format.</p> <p>Default: 3gpp</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 653• Configuring Persistent Storage on page 222• Configuring Charging on page 219 |

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] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | Specify a private extension (string) that gets appended to the filenames. |




NOTE: The file-naming 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*—*Host_Name_Gateway_Name*
- *RC*—A running counter, starting with 1
- *date*—Date when the CDR file was closed in YYYYMMDD format
- *time*—Time when the CDR file was closed in HHMMshhmm format
- *PI*—Optional private extension
- *FE*—Optional file extension

| | |
|---------------------------------|--|
| Options | <i>string</i> —Private extension Range: 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 653 • Configuring Persistent Storage on page 222 • Configuring Charging on page 219 |

file-size

| | |
|---------------------------------|---|
| Syntax | <code>file-size value;</code> |
| Hierarchy Level | [edit unified-edge gateways ggsn-pgw gateway-name charging local-persistent-storage-options] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>The files containing the CDRs are copied from a temporary location on the RE disk to a final location within the same RE disk, from where these files can be SFTP transferred. However, any one of the following conditions must be met (whichever comes first):</p> <ul style="list-style-type: none">• The size of the file reaches the configured or default limit.• The age 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> |
| | <p>Using this statement, you can configure the maximum size the file can reach, in MB, after which the CDR file is closed and copied to a final location within the same disk (<code>/opt/mobility/charging/ggsn/final_log</code>) from where it can be transferred via SFTP. The files thus transferred from the final location should be deleted from the local RE disk after the transfer. Only authorized users can perform this operation.</p> |
| Options | <p><i>value</i>—The maximum size the CDR file can reach, in MB, after which it is closed and copied to a final location within the RE disk, from where it can be SFTP transferred.</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 653• Configuring Persistent Storage on page 222• Configuring Charging on page 219 |

gtp

```
Syntax  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;
        reconnect-time duration;
        source-interface interface-name [ipv4-address address];
        t3-response response-interval;
        transport-protocol (tcp | udp);
        version (v0 | v1 | v2);
        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);
        }
    }
```

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name* charging]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description 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 there is no separate configuration defined for a peer, then the global configurations apply for that peer.

The Charging Data Function (CDF) sends the Charging Data Records (CDRs) as GTP Prime messages to the GTP Prime peer, based on this configuration.

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

- [charging on page 624](#)
- [Configuring GTP Prime for Charging on page 220](#)
- [Configuring GTP Prime Peers on page 221](#)

- [Configuring Charging on page 219](#)

header-type

| | |
|---------------------------------|---|
| Syntax | header-type (long short); |
| 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>] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>Configure the CDF GTP Prime message header length to match the version supported on the 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 short header length only.</p> <p>When there are global-level and peer-level configurations, the peer-level configuration takes precedence.</p> |
| Options | <p>long—CDF GTP Prime message header length is set to 20 bytes.</p> <p>short—CDF GTP Prime message header length is set to 6 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">• gtp on page 651• peer on page 660• Configuring GTP Prime for Charging on page 220• Configuring GTP Prime Peers on page 221• Configuring Charging on page 219 |

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]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description You typically store the Charging Data Records (CDRs) on the local Routing Engine (RE) 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 Service PICs are routed to a file on the RE disk. The statements in this hierarchy enable you to configure the CDR file storage options, thereby helping you to take measures to prevent any loss to the CDR data. To list a few of the configurable options:

- 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—The CDRs are routed to the files based on the file-routing criteria of the transport profile. So, all the 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**
- [charging on page 624](#)
 - [Configuring Persistent Storage on page 222](#)
 - [Configuring Charging on page 219](#)

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] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | Configure the RE disk as backup storage for the CDRs when the external storage resources (CGF servers) are down or if you do not have any external servers configured. |
| Options | Default: 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 664• Configuring Persistent Storage on page 222• Configuring Charging on page 219 |

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] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>Configure the maximum transmission unit (MTU) for a 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 CDRs is transmitted from the CDF to the 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 | <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 627 • Configuring Transport Profiles on page 226 • Configuring Charging on page 219 |

n3-requests

| | |
|---------------------------------|---|
| Syntax | <code>n3-requests requests;</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>] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>Configure the maximum number of times the CDF attempts to send echo request messages to the 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 mobile broadband gateway re-transmits the requests to the UDP peers. However, for the TCP peers, the requests are re-transmitted to a newer peer (when there is a switch-over) 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 | 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 651• peer on page 660• Configuring GTP Prime for Charging on page 220• Configuring GTP Prime Peers on page 221• Configuring Charging on page 219 |

no-path-management

| | |
|----------------------------|--|
| 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>] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | Use this statement to disable path management messages. If this 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 CDF and 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 651 • peer on page 660 • Configuring GTP Prime for Charging on page 220 • Configuring GTP Prime Peers on page 221 • Configuring Charging on page 219 |

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; peer charging-gateway-peer-name; peer charging-gateway-peer-name; } persistent-storage-order { local-storage; } switch-back-time seconds; } }</pre> |
| Hierarchy Level | [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i>] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| 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 CDRs that can be added to a DRT message.• The maximum transmission unit of a DRT message.• The generated CDRs to be compliant with a specific 3GPP release.• The duration the 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 RE disk for CDR storage. <p>The 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 681• Configuring Transport Profiles on page 226• Configuring Charging on page 219 |

offline (Trigger profiles)

```
Syntax  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);
        }
    }
```

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name* charging trigger-profiles *profile-name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description You can set a limit for the attributes that fall within this hierarchy, which when reached triggers charging updates for offline charging records.

For example, you can set the maximum duration that the 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 S-GW or SGSN that can occur before the CDR is updated and closed.

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

- [trigger-profiles on page 684](#)
- [Configuring Charging Trigger Events on page 227](#)
- [Configuring Charging on page 219](#)

peer (GTP Prime)

Syntax `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);
 }`

Hierarchy Level [edit unified-edge gateways ggsn-pgw gateway-name charging gtp]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure GTP Prime peers (CGF servers). You can configure up to a maximum of 24 peers.
The CDF sends the CDRs as GTP Prime messages to the GTP Prime peer, based on this configuration.
When there are global-level and peer-level configurations, the peer-level configuration takes precedence.

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

- [gtpp on page 651](#)
- [Configuring GTP Prime Peers on page 221](#)
- [Configuring GTP Prime for Charging on page 220](#)
- [Configuring Charging on page 219](#)

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] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | 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 the following statement). If not, you will encounter a configuration error. set unified-edge gateways ggsn-pgw <i>gateway-name</i> charging gtp peer |
| 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 662 • Configuring GTP Prime Peers on page 221 • Configuring GTP Prime for Charging on page 220 • Configuring Charging on page 219 |

peer-order

Syntax `peer-order {
 peer charging-gateway-peer-name;
 peer charging-gateway-peer-name;
 peer charging-gateway-peer-name;
 }`

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name* charging transport-profiles *profile-name*
 offline charging-gateways]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the CGF servers. You can configure up to a maximum of three servers for a transport profile.

When multiple CGF servers are available for storing CDRs, the 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 point of time, the CDRs are sent to only one of the peers and not to all. If for any reason this server goes **Down**, 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.

When required, the priority of any peer can be changed by using the configuration option to **insert before** or **insert after** the existing peers.



NOTE: If all the peers are Down and if you have configured the RE disk as the backup storage option, then the CDRs are routed to the RE 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 RE disk are not routed to the charging gateway (peer) and continue to remain on the disk. You need to SFTP it from the `/opt/mobility/charging/ggsn/final_log` location on the disk.

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

- [charging-gateways on page 627](#)
- [Configuring GTP Prime Peers on page 221](#)
- [Configuring GTP Prime for Charging on page 220](#)
- [Configuring Charging on page 219](#)


pending-queue-size

| | |
|---------------------------------|---|
| Syntax | <code>pending-queue-size <i>value</i>;</code> |
| Hierarchy Level | [edit unified-edge gateways <i>ggsn-pgw gateway-name</i> charging <i>gtp</i>] [edit unified-edge gateways <i>ggsn-pgw gateway-name</i> charging <i>gtp</i> peer <i>peer-name</i>] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>Configure the maximum number of Data Record Transfer (DRT) messages that can be sent by the CDF without an acknowledgement from the 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><i>value</i>—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 651 • peer on page 660 • Configuring GTP Prime Peers on page 221 • Configuring GTP Prime for Charging on page 220 • Configuring Charging on page 219 |

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] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>Configure the local storage of CDRs. You may want to store the CDRs on the local RE 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 | 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 627• Configuring Transport Profiles on page 226• Configuring Charging on page 219 |

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> |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| 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 S-GW, 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 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 right charging profile for that subscriber. However, if a server returns an incorrect or un-configured 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 | <p><i>id-num</i>—A unique number to be associated with a charging profile.</p> <p>Range: 1 through 65534</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-profiles on page 628 • Configuring Charging Profiles on page 231 • Charging Profiles on page 217 • Configuring Charging on page 219 |

reconnect-time

| | |
|---------------------------------|--|
| Syntax | <code>reconnect-time <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>] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>Configure the duration (in seconds) that the CDF must wait before trying to re-connect to a 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 re-connect 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 re-connect 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 651• peer on page 660• Configuring GTP Prime Peers on page 221• Configuring GTP Prime for Charging on page 220• Configuring Charging on page 219 |

service-mode (Charging Profiles)

| | |
|---------------------------------|---|
| Syntax | <code>service-mode maintenance;</code> |
| Hierarchy Level | <code>[edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i>]</code> |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>Put 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 under maintenance mode:</p> <ul style="list-style-type: none"> • Changing the CDR profile, transport profile, or the trigger profile associated with this charging profile • Changing the profile-id configuration • Deleting the charging profile <p>In maintenance mode, no new subscribers are accepted for that charging profile. However, the maintenance mode does not become active until there are no existing subscriber sessions using that charging profile and all their 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. You can use the following commands to help you with the maintenance-mode tasks:</p> <ul style="list-style-type: none"> • To verify whether the charging profile has entered active maintenance-mode, use: <code>show unified-edge ggsn-pgw charging service-mode gateway <i>gateway-name</i> charging-profile <i>profile-name</i></code> • To verify whether the subscriber count has reached zero, use: <code>show unified-edge ggsn-pgw subscribers charging charging-profile <i>profile-name</i> gateway <i>gateway-name</i></code> • To verify whether all CDRs for the transport profile referred to by this charging profile have been flushed out, use: <code>show unified-edge ggsn-pgw charging transfer status transport-profile-name <i>profile-name</i></code> • To explicitly end any subscriber sessions, use the following clear command: <code>clear unified-edge ggsn-pgw subscribers charging charging-profile <i>profile-name</i> gateway <i>gateway-name</i></code> • To explicitly flush all the CDRs for the transport profile referred to by this charging profile, use the following clear command: <code>clear unified-edge ggsn-psgw charging cdr transport-profile-name <i>profile-name</i></code> |
| 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 628 • Changing a Charging Profile on page 326 |

- [Mobility Maintenance Mode Overview on page 318](#)

service-mode (Transport Profiles)

| | |
|---------------------------------|---|
| Syntax | <code>service-mode maintenance;</code> |
| Hierarchy Level | [edit unified-edge gateways <i>ggsn-pgw gateway-name</i> charging transport-profiles <i>profile-name</i>] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>Put the respective transport profile under maintenance mode.</p> <p>When you have to make the following changes to the existing transport profile configuration, you must put that transport profile under maintenance mode:</p> <ul style="list-style-type: none"> • Changing the CDR encoding format to comply with a different 3GPP technical specification release (that is, changing the cdr-release configuration) • Deleting 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 there are no existing subscriber sessions using that transport profile and all their 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. You can use the following commands to help you with the maintenance-mode tasks:</p> <ul style="list-style-type: none"> • To verify whether the transport profile has entered active maintenance-mode, use: show unified-edge ggsn-pgw charging service-mode gateway <i>gateway-name</i> transport-profile <i>profile-name</i> • To verify whether the subscriber count has reached zero, use: show unified-edge ggsn-pgw subscribers charging transport-profile <i>profile-name</i> gateway <i>gateway-name</i> • To verify whether all CDRs for the transport profile have been flushed out, use: show unified-edge ggsn-pgw charging transfer status transport-profile-name <i>profile-name</i> • To explicitly end any subscriber sessions, use the following clear command: clear unified-edge ggsn-pgw subscribers charging charging-profile <i>profile-name</i> gateway <i>gateway-name</i> • To explicitly flush all the CDRs for the transport profile, use the following clear command: clear unified-edge ggsn-psgw charging cdr transport-profile-name <i>profile-name</i> |
| 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 681 • Changing a Transport Profile on page 327 • Mobility Maintenance Mode Overview on page 318 |

sgsn-sgw-change-limit

| | |
|---------------------------------|--|
| 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 SGSN or 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 659• Configuring Charging Trigger Events on page 227• Configuring Charging on page 219 |

source-interface

| | |
|---------------------------------|--|
| Syntax | <code>source-interface <i>interface-name</i> [<i>ipv4-address address</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> |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| 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 CGF servers. This is a mandatory configuration. However, before specifying this configuration, make sure that the interface has been previously defined.</p> <p>For example, the configuration will look something like:</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><i>address</i>—The IPv4 address of the local loopback interface from which the GTP Prime packets are sent. This is a mandatory configuration.</p> <p><i>interface-name</i>—The 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 651 • peer on page 660 • Configuring GTP Prime for Charging on page 220 • Configuring GTP Prime Peers on page 221 • Configuring Charging on page 219 |

switch-back-time

| | |
|----------------------------|--|
| Syntax | <code>switch-back-time <i>seconds</i>;</code> |
| Hierarchy Level | [edit unified-edge gateways <i>ggsn-pgw gateway-name</i> charging transport-profiles <i>profile-name</i> offline charging-gateways] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | The CDF transmits the CDRs to the peer, which is of highest priority. The priority is determined by the peer-order configuration. If for any reason this 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 RE 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 may want to configure the local storage on the RE disk using the following command:

```
set unified-edge gateways ggsn-pgw gateway-name charging transport-profiles profile-name offline charging-gateways persistent-storage-order local-storage
```

However, even if the RE disk is not configured for storage, the CDR data is not lost because it gets buffered in the Service PICs. Service 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 getting stored previously on the RE disk are not routed to the charging gateway (peer) and continue to remain on the disk. You need to SFTP it from the `/opt/mobility/charging/ggsn/final_log` location on the disk.

| | |
|---------------------------------|--|
| Options | <code><i>seconds</i></code> —Time, in seconds, CDF waits before transmitting the CDRs to the highest priority peer. Range: 0 through 300 seconds Default: 30 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">• charging-gateways on page 627• Configuring Transport Profiles on page 226 |

- [Configuring Charging on page 219](#)

t3-response

| | |
|---------------------------------|--|
| Syntax | <code>t3-response response-interval;</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>] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | Configure the duration (in seconds) that the CDF must wait before resending a GTP Prime message when the response to a request has not been received. When there are global-level and peer-level configurations, the peer-level configuration takes precedence. |
| Options | <i>response-interval</i> —Time that the CDF waits before resending a GTP Prime message when the response to a request has not been received. Range: 1 through 5 seconds Default: 5 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"> • gtp on page 651 • peer on page 660 • Configuring GTP Prime for Charging on page 220 • Configuring GTP Prime Peers on page 221 • Configuring Charging on page 219 |


tariff-time-list

| | |
|---------------------------------|--|
| Syntax | <pre>tariff-time-list { <i>tariff-time</i>; }</pre> |
| Hierarchy Level | [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i>] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>Configure a list of local times (in hh:mm format) at which the tariff changes and CDRs must be 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 among these values. You can configure up to a maximum of 24 values.</p> <p>Any change to the existing configuration applies to both existing as well as any new subscriber sessions.</p> |
| Options | <i>tariff-time</i> —Local time at which you want 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 684• Configuring Charging Trigger Events on page 227• Configuring Charging on page 219 |

time-limit

| | |
|---------------------------------|--|
| Syntax | <code>time-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 | <p>Configure the duration in seconds (since the previous trigger) after which the CDR is updated with the uplink and downlink bytes transmitted in this duration and is closed. For example, if the value is set to 3600 seconds, then the total resource utilization for the past 1 hour is added to the CDR and the CDR is closed.</p> <p>Any change to the existing configuration does not have impact on a previously established session. The updated configuration applies only to the new sessions.</p> |
| Options | <p><i>value</i>—Duration in seconds.</p> <p>Range: 600 through 65,535 seconds</p> <p>Default: 0. No time-limit is set 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"> • offline on page 659 • Configuring Charging Trigger Events on page 227 • Configuring Charging on page 219 |

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 the -ms#fic#pic term to the filename and places the file in the /var/log directory. For example, if you have configured the filename to be smd, then the actual log filename that you see on the router is, smd-ms#fic#pic (ms in the filename stands for the multi service card).</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 style="display: flex; align-items: center;">  <div style="margin-left: 10px;"> <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.</p> </div> </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, which 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 IPC between mobile-smd and chargemand.
- **path-management**—Trace path management operations within the path manager module within chargemand.
- **resource**—Trace resources, such as memory, counters, and so on.
- **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 Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [charging on page 624](#)
- [Tracing Charging Operations on page 233](#)

traceoptions (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 | [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging local-persistent-storage-options] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | Specify tracing options related to the storage of CDRs on the local RE disk. |
| Options | <p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. The router appends the -ms#fic#pic term to the filename and places the file in the /var/log directory. For example, if you have configured the filename to be localstorage, then the actual log filename that you see in the router is, localstorage-ms#fic#pic (ms in the filename stands for the multi service card).</p> <p>Range: 1 through 1024 bytes</p> <p>files <i>number</i>—(Optional) Maximum number of trace files. When a trace file named <i>trace-file</i> reaches its maximum size, it is renamed <i>trace-file.0</i>, then <i>trace-file.1</i>, 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 style="display: flex; align-items: center;">  <div style="margin-left: 10px;"> <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.</p> </div> </div> | |
| <ul style="list-style-type: none"> • all—Trace all operations. • connection—Trace the connection establishment between RE and all Service 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 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.

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 653 |
| | • Configuring Persistent Storage on page 222 |

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> |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| 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 (RE) disk, or both.</p> <p>Any modification to the existing configuration of this attribute must be done only when the charging-profile to which it is associated is under active maintenance mode. Use the following command to bring the charging profile under maintenance mode:</p> <p><code>set unified-edge gateways ggsn-pgw <i>gateway-name</i> charging charging-profiles <i>profile-name</i> service-mode maintenance</code></p> <div><p>TIP: If the profile has not been defined previously, use the following command to define a new transport profile:</p><p><code>set unified-edge gateways ggsn-pgw <i>gateway-name</i> charging transport-profiles <i>profile-name</i></code></p></div> |
| Options | <i>profile-name</i> —Name of the transport 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 628• Configuring Charging Profiles on page 231• Charging Profiles on page 217• Configuring Charging on page 219 |


transport-profiles

| | |
|---------------------------------|--|
| Syntax | <pre> transport-profiles <i>profile-name</i> { <i>description string</i>; offline { charging-gateways { <i>cdr-aggregation-limit value</i>; <i>cdr-release</i> (r7 r8 r99); <i>mtu value</i>; peer-order { <i>peer charging-gateway-peer-name</i>; <i>peer charging-gateway-peer-name</i>; <i>peer charging-gateway-peer-name</i>; } persistent-storage-order { <i>local-storage</i>; } <i>switch-back-time seconds</i>; } } <i>service-mode</i> maintenance; } </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 | <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 (RE) 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 624 • Configuring Transport Profiles on page 226 • Configuring Charging on page 219 |

transport-protocol

| | |
|---------------------------------|--|
| Syntax | transport-protocol (tcp udp); |
| 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>] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>Configure the transport protocol for transmitting the GTP Prime packets from CDF to the 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>tcp—The transport protocol used is tcp.</p> <p>udp—The transport protocol used is udp.</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 651• peer on page 660• Configuring GTP Prime for Charging on page 220• Configuring GTP Prime Peers on page 221• Configuring Charging on page 219 |

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> |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>Associate a trigger 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 trigger profile configuration associated with this profile determines the events that result in the creation of a CDR, addition of a container to a CDR, and the closure of a CDR.</p> <div style="display: flex; align-items: flex-start;">  <div> <p>TIP: If the profile has not been defined previously, use the following command to define a new trigger profile:</p> <pre>set unified-edge gateways ggsn-pgw <i>gateway-name</i> charging trigger-profiles <i>profile-name</i></pre> </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 628 • Configuring Charging Profiles on page 231 • Charging Profiles on page 217 • Configuring Charging on page 219 |

trigger-profiles

```
Syntax  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;
        }
    }
```

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name* charging]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

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 CGF server.

The remaining statements are explained separately.

Options *profile-name*—Name of the trigger profile.

Range: 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 624](#)
- [Configuring Charging Trigger Events on page 227](#)

- [Configuring Charging on page 219](#)

user-name

| | |
|---------------------------------|--|
| Syntax | <code>user-name <i>string</i>;</code> |
| Hierarchy Level | [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging local-persistent-storage-options] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>Restrict access to the CDR files to a specific user.</p> <p>The root user always has access permissions in addition to the non-root user that you have authorized, using this command.</p> |
| Options | <p><i>string</i>—User name.</p> <p>Range: 1 through 32 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">• local-persistent-storage-options on page 653• Configuring Persistent Storage on page 222• Configuring Charging on page 219 |

version

| | |
|---------------------------------|---|
| Syntax | version (v0 v1 v2); |
| 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>] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| 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 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—The GTP Prime version supported is v0.</p> <p>v1—The GTP Prime version supported is v1.</p> <p>v2—The GTP Prime version supported is v2.</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 651• peer on page 660• Configuring GTP Prime for Charging on page 220• Configuring GTP Prime Peers on page 221• Configuring Charging on page 219 |

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] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>Configure the volume of data (in bytes) that you want to transmit (since the previous trigger) before the CDR is updated with the transmitted uplink and downlink bytes and is closed. In addition, you can specify whether the maximum volume of data transmitted should include the data transmitted in both the uplink and downlink directions or only the uplink direction.</p> <p>Any change to the existing configuration does not have impact on a previously established session. The updated configuration applies only to the new sessions.</p> |
| Options | <p><i>value</i>—Maximum volume of data transmitted, in bytes, after which the CDR is updated and closed.</p> <p>Range: 1 through 4 GB</p> <p>Default: There is no default volume limit; that is, by default, the volume-limit trigger is disabled.</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 659 • Configuring Charging Trigger Events on page 227 • Configuring Charging on page 219 |

watermark-level-1

| | |
|---------------------------------|---|
| Syntax | <code>watermark-level-1 (notification-level (both snmp-alarm syslog)) (percentage <i>value</i>);</code> |
| Hierarchy Level | [edit unified-edge gateways <i>ggsn-pgw gateway-name</i> charging local-persistent-storage-options disk-space-policy] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | Configure the percentage of RE 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 do both. You can then take appropriate measures to prevent any loss of CDR data. |
| Options | <p>notification-level (both snmp-alarm syslog)—Specify whether you want to raise snmp alarms or log information on the system logs, or do 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>—The percentage of RE disk space to be used for storage after which you get an alert (if it is configured).</p> <p>Default: 70% of the RE disk space</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">• disk-space-policy on page 636• Configuring Persistent Storage on page 222• Configuring Charging on page 219 |

watermark-level-2

| | |
|---------------------------------|---|
| Syntax | <code>watermark-level-2 (notification-level (both snmp-alarm syslog)) (percentage <i>value</i>);</code> |
| Hierarchy Level | [edit unified-edge gateways <i>ggsn-pgw gateway-name</i> charging local-persistent-storage-options disk-space-policy] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | Configure the percentage of RE 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 do both. You can then take appropriate measures to prevent any loss of CDR data. |
| Options | <p>notification-level (both snmp-alarm syslog)—Specify whether you want to raise snmp alarms or log information on the system logs, or do 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>—The percentage of RE disk space to be used for storage after which you get an alert (if it is configured).</p> <p>Default: 80% of the RE disk space</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"> • disk-space-policy on page 636 • Configuring Persistent Storage on page 222 • Configuring Charging on page 219 |

watermark-level-3

| | |
|---------------------------------|---|
| Syntax | <code>watermark-level-3 (notification-level (both snmp-alarm syslog)) (percentage <i>value</i>);</code> |
| Hierarchy Level | [edit unified-edge gateways <i>ggsn-pgw gateway-name</i> charging local-persistent-storage-options disk-space-policy] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>Configure the percentage of RE 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 do both.</p> <p>When this watermark level is reached, the Charging daemon stops writing the CDRs to the local RE disk till the CDR storage space is restored by transferring the files via SFTP and deleting the files from the CDR log directory. However, the data is not immediately lost because the Service 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 or log information on the system logs, or do 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>—The percentage of RE disk space to be used for storage after which you get an alert (if it is configured).</p> <p>Default: 90% of the RE disk space</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">• disk-space-policy on page 636• Configuring Persistent Storage on page 222• Configuring Charging on page 219 |

world-readable

| | |
|---------------------------------|--|
| Syntax | world-readable; |
| Hierarchy Level | [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> charging local-persistent-storage-options] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | Allow all users to have read permission on the 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 653• Configuring Persistent Storage on page 222• Configuring Charging on page 219 |

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 | <p>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.</p> |
| Options | <p><i>downlink</i>—Aggregated maximum bit rate for downlink traffic.</p> <p><i>reject</i>—Aggregated maximum bit rate to be rejected.</p> <p><i>uplink</i>—Aggregated maximum bit rate for uplink traffic.</p> <p><i>upgrade</i>—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 253 • cos-policy-profiles on page 703 |

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 253• cos-policy-profiles on page 703 |

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 253 • cos-cac on page 700 |

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 | 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 253• resource-threshold-profiles on page 721 |

classifier-profile

| | |
|---------------------------------|---|
| Syntax | 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. 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 253• local-policies on page 712 |

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 | 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. |
| Default | If you do not configure any CoS features, all packets are transmitted from the output transmission queue 0. |
| Options | <p><i>profile-name</i>—Name of the classifier profile to be applied to this 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 QoS on the Broadband Gateway Overview on page 253• cos-cac on page 700 |

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 | <p>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.</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 253 |

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 253 |

cos-policy-profile

| | |
|---------------------------------|---|
| Syntax | <code>cos-policy-profile <i>name</i> ;</code> |
| 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. 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 253• local-policies on page 712 |

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 253 |

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 | <i>high</i> —High threshold configuration. <i>low</i> —Low threshold 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 QoS on the Broadband Gateway Overview on page 253• resource-threshold-profiles on page 721 |

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 253 • local-policies on page 712 |

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 253 • rewrite-rules on page 723 |

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 253• ingress-rewrite-rules on page 710 |

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 253• rewrite-rules on page 723 |

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 253 • ingress-rewrite-rules on page 710 |

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 253 • cos-policy-profiles on page 703 |

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 253• cos-policy-profiles on page 703 |

high

| | |
|---------------------------------|---|
| Syntax | high { gtpv1-arp <i>y</i> ; gtpv2-priority-level <i>z</i> ; percentage <i>x</i> ; } |
| 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 | <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 253 • bearer-load on page 696 |

inet-precedence

| | |
|---------------------------------|--|
| Syntax | inet-precedence <i>rewrite-rule-name</i> [protocol gtp-inet-both gtp-inet-outer]; |
| 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 | <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 253 • rewrite-rules on page 723 |

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 253• ingress-rewrite-rules on page 710 |

ingress-rewrite-rules

| | |
|---------------------------------|--|
| Syntax | <pre>ingress-rewrite-rules { <i>dscp</i> <i>rewrite-rule-name</i>; <i>dscp-ipv6</i> <i>rewrite-rule-name</i>; <i>inet-precedence</i> <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 253• interfaces on page 711 |


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 | <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 253 • class-of-service on page 699 |

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 | 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. |
| 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 253 |

local-policy-profile (MobileNext Broadband Gateway)

| | |
|---------------------------------|--|
| Syntax | <code>local-policy-profile <i>local-policy-profile</i>;</code> |
| Hierarchy Level | [edit unified-edge gateways ggsn-pgw <i>gateway-name</i>] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | Specify a local policy for 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). |
| | <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 583 |

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 | 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 253• bearer-load on page 696 |

maximum-bearers (MobileNext Broadband Gateway)

| | |
|---------------------------------|---|
| Syntax | <code>maximum-bearers <i>maximum-bearers</i>;</code> |
| Hierarchy Level | [edit unified-edge gateways ggsn-pgw <i>gateway-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 broadband gateway. |
| Default | If you do not configure the maximum-bearers , then the default value of 12,000,000 is used. |
| Options | <i>maximum-bearers</i> —Maximum number of bearers for the broadband gateway. 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">• Configuring the Maximum Number of Bearers on page 254• maximum-bearers (APN) on page 585 |

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 | The remaining statements are explained separately. Range: 1 through 256,000 Kbps. |
| 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 253• cos-policy-profiles on page 703 |


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 253 • resource-threshold-profiles on page 721 |

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 253 |

preemption (MobileNext Broadband Gateway)

| | |
|---------------------------------|---|
| 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 broadband gateway. 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 allocation and retention priority (ARP) level 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 ARP 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 broadband gateway. 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 256 |

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 253• cos-policy-profiles on page 703• classifier-profiles on page 698 |

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 253• cos-cac on page 700 |

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 253• local-policies on page 712 |

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 253 • interfaces on page 711 |

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 253 • local-policies on page 712 |

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 253• local-policies on page 712 |

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 253 • resource-threshold-profiles on page 721 |

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 | <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 253• classifier-profiles on page 698 |

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 253 • cos-policy-profiles on page 703 |

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 253• local-policies on page 712 |

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 253• cos-policy-profiles on page 703 |

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 253 • local-policies on page 712 |

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 253 • local-policies on page 712 |

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 68 • Example: Configuring Broadband Gateway Exception Handling Parameters on page 72 • ipv6-router-advertisement (MobileNext Broadband Gateway) on page 735 |

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 68• Example: Configuring Broadband Gateway Exception Handling Parameters on page 72• ipv6-router-advertisement (MobileNext Broadband Gateway) on page 735 |

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 192• Example: Configuring Broadband Gateway Exception Handling Parameters on page 72• data on page 752 |

ip-reassembly

| | |
|---------------------------------|---|
| Syntax | <pre>ip-reassembly <i>profile-name</i> { max-reassembly-pending-packets <i>number</i>; timeout <i>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 66• Example: Configuring Broadband Gateway Exception Handling Parameters on page 72 |

ip-reassembly-profile

Syntax `ip-reassembly-profile {
 profile-name;
 }`

Hierarchy Level `[edit unified-edge gateways ggsn-pgw gateway-name]`

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Apply a previously configured IP reassembly profile to the broadband gateway.



.....
NOTE: Currently, only one IP reassembly profile is allowed for the broadband gateway.
.....

Options `profile-name`—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

- [\[edit unified-edge gateways\] Hierarchy Level on page 456](#)
- [Configuring Fragment Reassembly Parameters on page 66](#)
- [Example: Configuring Broadband Gateway Exception Handling Parameters on page 72](#)

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] Hierarchy Level on page 456 • Configuring IPv6 Protocol Parameters on page 68 • Example: Configuring Broadband Gateway Exception Handling Parameters on page 72 |

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 66• Example: Configuring Broadband Gateway Exception Handling Parameters on page 72• ip-reassembly on page 733 |

maximum-advertisement-interval (IPv6 Router Advertisement)

| | |
|---------------------------------|--|
| Syntax | <code>maximum-advertisement-interval <i>maximum-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 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><i>maximum-advertisement-interval</i>—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 68• Example: Configuring Broadband Gateway Exception Handling Parameters on page 72• ipv6-router-advertisement (MobileNext Broadband Gateway) on page 735 |

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 68• Example: Configuring Broadband Gateway Exception Handling Parameters on page 72• ipv6-router-advertisement (MobileNext Broadband Gateway) on page 735 |

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 68 • Example: Configuring Broadband Gateway Exception Handling Parameters on page 72 • ipv6-router-advertisement (MobileNext Broadband Gateway) on page 735 |

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 68• Example: Configuring Broadband Gateway Exception Handling Parameters on page 72• ipv6-router-advertisement (MobileNext Broadband Gateway) on page 735 |

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 68 • Example: Configuring Broadband Gateway Exception Handling Parameters on page 72 • ipv6-router-advertisement (MobileNext Broadband Gateway) on page 735 |

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 68• Example: Configuring Broadband Gateway Exception Handling Parameters on page 72• ipv6-router-advertisement (MobileNext Broadband Gateway) on page 735 |

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 68 • Example: Configuring Broadband Gateway Exception Handling Parameters on page 72 • ipv6-router-advertisement (MobileNext Broadband Gateway) on page 735 |

software-datapath

Syntax `software-datapath {
 traceoptions {
 file filename {
 files files;
 match match;
 size size;
 (no-world-readable | world-readable);
 }
 flag {
 flag;
 }
 level level;
 no-remote-trace;
 }
 }`

Hierarchy Level `[edit unified-edge gateways ggsn-pgw gateway-name]`

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

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

- [\[edit unified-edge gateways\] Hierarchy Level on page 456](#)
- [Configuring Exception Handling Traceoptions on page 70](#)

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 66• Example: Configuring Broadband Gateway Exception Handling Parameters on page 72• ip-reassembly on page 733 |

traceoptions (Exception Handling)

Syntax `traceoptions {
 file filename {
 files files;
 match match;
 size size;
 (no-world-readable | world-readable);
 }
 flag {
 flag;
 }
 level level;
 no-remote-trace;
 }`

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name* software-datapath]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Define tracing operations for exception handling.

Options **file *filename***—Name of the file that receives the output of the tracing operation. All files are placed in the `/var/log` directory.

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:
 - **ager**—Trace flow ageout-related events.
 - **all**—Trace everything.
 - **commands**—Trace operational commands.
 - **configuration**—Trace configuration commands.
 - **flow**—Trace flow.
 - **commands**—Trace operational commands.
 - **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 | <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 Exception Handling Traceoptions on page 70 • software-datapath on page 744 |

Gateway Maintenance Mode Configuration Statement

service-mode (Gateways)

| | |
|---------------------------------|---|
| 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 782• Mobility Maintenance Mode Overview on page 318 |

GTP Configuration Statements

control

Syntax

```
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 [ip-address];
  n3-requests requests;
  path-management (enable | disable);
  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 signaling and control 3GPP parameters. These parameters are applicable to the 3GPP interface such as S5, S8, Gn, Gp, and so on, under which the signaling and control parameters are configured. The parameters configured are common and apply across all GTP peers that connect to the interface. For example, the control configuration block may have the following parameters: **n3-requests**, **t3-response**, 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 GTP Services Overview on page 186](#)
- [gtp on page 758](#)

data

| | |
|---------------------------------|--|
| 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>; interface <i>interface-name</i> <i>v4-address</i> [<i>ip-address</i>]; n3-requests <i>requests</i>; path-management (enable disable); 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 the 3GPP data-forwarding parameters. These parameters are applicable to the 3GPP interface such as S5, S8, Gn, Gp, and so on, under which the data parameters are configured. The parameters configured are common and apply across all GTP peers that connect to the interface. For example, the data configuration block may have the following parameters: n3-requests , t3-response , 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 GTP Services Overview on page 186• gtp on page 758 |

dscp-code-point

| | |
|---------------------------------|---|
| Syntax | <pre>dscp-code-point <i>value</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 | Specify the value of the Differentiated Services (DiffServ) field within the IP header. The DSCP code point is exclusively used for GTP messages. |
| Options | value —DSCP code point value. |
| 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 186• gtp on page 758 |

echo-interval

| | |
|---------------------------------|--|
| Syntax | <code>echo-interval <i>interval</i>;</code> |
| 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 the echo request interval value for path management. The echo request interval value is the number of seconds that the gateway (P-GW/PDN-GW) waits before sending an echo-request message to the peer (SGSN, S-GW or Charging Gateway). This interval applies to both GTP-C and GTP-U echo messages unless datapath-echo-interval is configured explicitly. |
| Default | If you do not include this statement, the value of the interval is set to 60 seconds. |
| Options | interval — Number of seconds that the gateway waits before sending an echo-request message to the peer. Range: 60 through 65535 seconds. |
| Required Privilege Level | interface—To view this statement in the configuration. interface-control—To add this statement to the configuration. |

echo-n3-requests

| | |
|---------------------------------|--|
| Syntax | <code>echo-n3-requests <i>requests</i>;</code> |
| 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 the number of retries of GTP echo messages on timeout. The echo-n3-requests indicates the number of attempts for GTP echo requests. This occurs only when there is no response as indicated in the echo-t3-response. |
| Default | If you do not include this statement, the value of echo-n3-requests is set to 3. |
| Options | requests —Maximum number of times that the broadband gateway attempts to send a signaling-request message. Range: 1 through 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 GTP Services Overview on page 186 • gtp on page 758 |

echo-t3-response

| | |
|---------------------------------|---|
| Syntax | <code>echo-t3-response <i>response-interval</i>;</code> |
| 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 the response timeout value for a GTP echo-request message. The echo-t3-response indicates the time (in seconds) duration for the system to receive an echo response for the transmitted echo requests. |
| Default | If you do not include this statement, the T3 response interval is set to 5 seconds. |
| Options | <i>response interval</i> —Time (seconds) that the gateway waits before resending a signaling-request message. Range: 1 through 65,535 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 186• gtp on page 758 |

error-indication-interval

| | |
|---------------------------------|---|
| Syntax | <code>error-indication-interval <i>seconds</i>;</code> |
| 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 the minimum interval for indicating an error per bearer. This interval decides the number of times an error can be indicated. |
| Default | If you do not include this statement, the value of the interval is set to 1 second. |
| Options | <i>seconds</i> — Number of seconds that the gateway waits before indicating an error message to the peer. Range: 1 through 20 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 186• gtp on page 758 |

forwarding-class

| | |
|---------------------------------|---|
| Syntax | <code>forwarding-class <i>class-name</i>;</code> |
| Hierarchy Level | [edit unified-edge gateways ggsn-pgw <i>name</i> gtp] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | Define the forwarding class name and option values for the classification of host traffic to the forwarding engine. |
| Options | <i>class-name</i> —Name of the forwarding class. |
| 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 186• gtp on page 758 |

gn

```

Syntax  gn {
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        interface interface-name v4-address [ip-address];
        n3-requests requests;
        path-management (enable | disable);
        t3-response response-interval;
        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 [ip-address];
            n3-requests requests;
            path-management (enable | disable);
            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 [ip-address];
            n3-requests requests;
            path-management (enable | disable);
            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 3GPP control and data parameter values applicable to the 3GPP Gn interface. The values configured here override the common control and data configuration. The parameters configured are common and apply across all GTP peers that connect to the interface. For example, the gn configuration block may have the following parameters: control, data, 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 GTP Services Overview on page 186](#)
- [gtp on page 758](#)

gp

```

Syntax  gp {
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        interface interface-name v4-address [ip-address];
        n3-requests requests;
        path-management (enable | disable);
        t3-response response-interval;
        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 [ip-address];
            n3-requests requests;
            path-management (enable | disable);
            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 [ip-address];
            n3-requests requests;
            path-management (enable | disable);
            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 3GPP control and data parameter applicable to the 3GPP gp interface. The values configured here override the common control and data configuration. The parameters configured are common and apply across all GTP peers that connect to the interface. For example, the gp configuration block may have the following parameters: control, data, 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 GTP Services Overview on page 186](#)
- [gtp on page 758](#)

gtp

```
Syntax  gtp {
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        n3-requests requests;
        path-management (enable | disable);
        t3-response response-interval;
        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 [ip-address];
            n3-requests requests;
            path-management (enable | disable);
            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 [ip-address];
            n3-requests requests;
            path-management (enable | disable);
            t3-response response-interval;
        }
        gn {
            echo-interval interval;
            echo-n3-requests requests;
            echo-t3-response response-interval;
            interface interface-name v4-address [ip-address];
            n3-requests requests;
            path-management (enable | disable);
            t3-response response-interval;
            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 [ip-address];
                n3-requests requests;
                path-management (enable | disable);
                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 [ip-address];
    n3-requests requests;
    path-management (enable | disable);
    t3-response response-interval;
  }
}
gp {
  echo-interval interval;
  echo-n3-requests requests;
  echo-t3-response response-interval;
  interface interface-name v4-address [ip-address];
  n3-requests requests;
  path-management (enable | disable);
  t3-response response-interval;
  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 [ip-address];
    n3-requests requests;
    path-management (enable | disable);
    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 [ip-address];
    n3-requests requests;
    path-management (enable | disable);
    t3-response response-interval;
  }
}
s5 {
  echo-interval interval;
  echo-n3-requests requests;
  echo-t3-response response-interval;
  interface interface-name v4-address [ip-address];
  n3-requests requests;
  path-management (enable | disable);
  t3-response response-interval;
  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 [ip-address];
    n3-requests requests;
    path-management (enable | disable);
    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 [ip-address];
    n3-requests requests;
    path-management (enable | disable);
    t3-response response-interval;
  }
}
s8 {
  echo-interval interval;
  echo-n3-requests requests;
  echo-t3-response response-interval;
  interface interface-name v4-address [ip-address];
  n3-requests requests;
  path-management (enable | disable);
  t3-response response-interval;
  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 [ip-address];
    n3-requests requests;
    path-management (enable | disable);
    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 [ip-address];
    n3-requests requests;
    path-management (enable | disable);
    t3-response response-interval;
  }
}
peer-groups peer-groups name {
  echo-interval interval;
  echo-n3-requests requests;
  echo-t3-response response-interval;
  n3-requests requests;
  path-management (enable | disable);
  peer (ip-address | ip-prefix);
  routing-instance routing-identifier;
  t3-response response-interval;
  control {
    sequence-number-length 16-bits;
  }
}
traceoptions {
  file filename <files number> <size size> ;
}

```



```

    flag flag (config | debug | decode | encode | events | packet-io | peer | tracker | warning |
    all) ;
    level (error | info | notice | verbose | warning | all) ;
  }
}

```

Hierarchy Level [edit unified-edge gateways ggsn-pgw]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description The GPRS tunneling protocol (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 SGSN or S-GW to which it is connected.

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 186](#)

interface

Syntax Interface *interface-name*;

Hierarchy Level [edit unified-edge gateways ggsn-pgw *name* gtp]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

Description Configure the interface name and IP address used for all 3GPP interfaces. You can configure the Gn, Gp, S5, and S8 interfaces for the broadband gateway.

Options *interface-name*—Name of the interface used in the gateway.

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 186](#)
- [gtp on page 758](#)

v4-address

| | |
|---------------------------------|---|
| Syntax | <code>interface <i>interface name</i> v4-address <i>ip-address</i>;</code> |
| 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 the IPv4 address for the interface. |
| Options | <i>interface-name</i> —Name of the interface for the gateway. <i>ip-address</i> —IPv4 address. |
| 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 186• gtp on page 758 |

n3-requests

| | |
|---------------------------------|--|
| Syntax | <code>n3-requests <i>requests</i>;</code> |
| Hierarchy Level | [edit unified-edge gateways ggsn-pgw <i>name</i> gtp] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | Number of retries of GTP request messages upon t3 timeout. Maximum number of times that the gateway (P-GW/PDN-GW) attempts to send a signaling-request to a peer (SGSN or S-GW). |
| Default | If you do not include this statement, the value of n3-requests is set to 3. |
| Options | <i>requests</i> — Maximum number of times that the gateway attempts to send a signaling-request message. Range: 1 through 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 GTP Services Overview on page 186• gtp on page 758 |

path-management

| | |
|---------------------------------|--|
| Syntax | <code>path-management (enable disable);</code> |
| Hierarchy Level | [edit unified-edge gateways ggsn-pgw <i>name</i> gtp] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | Enable or disable control or data path management. Path management is performed by GTP echo-request or echo-response messages. |
| 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 186 • gtp on page 758 |

peer

| | |
|---------------------------------|--|
| Syntax | <code>peer <i>ip-address</i> <i>ip-prefix</i>;</code> |
| 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 the 3GPP GTP peer IP address. Peer can also be a network (subnet). |
| Options | <p><i>ip-address</i>—IPv4 address.</p> <p><i>ip-prefix</i>—Prefix for the IP address.</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 186 • gtp on page 758 |

peer-groups

| | |
|---------------------------------|---|
| Syntax | <pre>peer-groups <i>peer-groups name</i> { <i>echo-interval interval</i>; <i>echo-n3-requests requests</i>; <i>echo-t3-response response-interval</i>; <i>n3-requests requests</i>; <i>path-management</i> (enable disable); <i>peer</i> (ip-address ip-prefix); <i>routing-instance routing-identifier</i>; <i>t3-response response-interval</i>; control { <i>sequence-number-length</i> 16-bits; } }</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 3GPP parameter values. This configuration overrides the 3GPP common or interface-specific configuration for a peer contained in the group. |
| Options | <p><i>control</i>—3GPP GTP peer group control plane options.</p> <p><i>peer</i>— Peer IP address 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">• Configuring GTP Services Overview on page 186• gtp on page 758 |

peer-history

| | |
|---------------------------------|---|
| Syntax | <code>peer-history <i>number</i>;</code> |
| 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 the maximum number of peers for which the system stores the historical values of message statistics and peer restarts. |
| Options | <i>number</i> —Number of peers to store historical value of messages. 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 186• gtp on page 758 |

routing-instance

| | |
|---------------------------------|--|
| Syntax | <code>routing-instance <i>routing-identifier</i>;</code> |
| 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 the routing instance or VPN routing and forwarding (VRF) for the peer group. VRF provides the ability to configure and maintain more than one instance of a routing and forwarding table within the same router. |
| Options | <i>routing-identifier</i> —Identifier value 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 186• gtp on page 758 |

s5

```

Syntax  s5 {
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        interface interface-name v4-address [ip-address];
        n3-requests requests;
        path-management (enable | disable);
        t3-response response-interval;
        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 [ip-address];
            n3-requests requests;
            path-management (enable | disable);
            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 [ip-address];
            n3-requests requests;
            path-management (enable | disable);
            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 3GPP control and data parameters applicable to the 3GPP s5 interface. The values configured here override the common control and data configuration. The parameters configured are common and apply across all GTP peers that connect to the interface. For example, the s5 configuration block may have the following parameters: control, data, 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 GTP Services Overview on page 186](#)
- [gtp on page 758](#)

s8

```

Syntax  s8 {
        echo-interval interval;
        echo-n3-requests requests;
        echo-t3-response response-interval;
        interface interface-name v4-address [ip-address];
        n3-requests requests;
        path-management (enable | disable);
        t3-response response-interval;
        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 [ip-address];
            n3-requests requests;
            path-management (enable | disable);
            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 [ip-address];
            n3-requests requests;
            path-management (enable | disable);
            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 3GPP control and data parameters applicable to the 3GPP s8 interface. The values configured here override the common control and data configuration. The parameters configured are common and apply across all GTP peers that connect to the interface. For example, the s8 configuration block may have the following parameters: control, data, 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 GTP Services Overview on page 186](#)
- [gtp on page 758](#)

sequence-number-length

| | |
|---------------------------------|---|
| Syntax | sequence-number-length 16-bits; |
| 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 support for 16-bit sequence numbers for GTPv2 signaling or control messages. |
| 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 186• gtp on page 758 |

t3-response

| | |
|---------------------------------|---|
| Syntax | t3 response <i>response-interval</i> ; |
| 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 the response timeout value for a GTP request message. The t3 response is the time duration for which the gateway waits before sending a signaling-request message when the response to a request has not been received. |
| Default | If you do not include this statement, the T3 response interval is set to 5 seconds. |
| Options | seconds —Time that the gateway waits before resending a signaling-request message. Range: 1 through 65,535 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 186• gtp on page 758 |

traceoptions

| | |
|---------------------------------|---|
| Syntax | <pre> traceoptions { file <i>filename</i> <files <i>number</i>> <size <i>size</i>> ; } flag <i>flag</i> (config debug decode encode events packet-io peer tracker warning all) ; level (error info notice verbose warning all); } </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 GTP tracing options. To specify more than one tracing operation, include multiple flag statements. |
| Options | <p>file—Trace the file information.</p> <p>flag—Tracing parameters, such as:</p> <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. |
| 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 186 • gtp on page 758 |

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 772 |

hash-keys (Aggregated Multiservices)

| | |
|----------------------------|--|
| Syntax | <pre>hash-keys { egress-key (destination-ip source-ip); ingress-key (destination-ip source-ip); }</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, and application-level gateway [ALG]). 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 45 on page 772 for the supported hash keys.</p> |

Table 45: 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 | <ul style="list-style-type: none"> • load-balancing-options (Aggregated Multiservices) on page 775 |

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 772 |

interface-service (Aggregated Multiservices)

Syntax `interface-service {
 load-balancing-options {
 hash-keys {
 egress-key (destination-ip | source-ip);
 ingress-key (destination-ip | source-ip);
 }
 }
 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, and application-level gateway [ALG]), 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 776](#)

load-balancing-options (Aggregated Multiservices)

| | |
|---------------------------------|---|
| Syntax | <pre>load-balancing-options { hash-keys { egress-key (destination-ip source-ip); ingress-key (destination-ip source-ip); } }</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, and application-level gateway [ALG]). 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 | <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"> • interface-service (Aggregated Multiservices) on page 774 |

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);
                }
            }
        }
        service-interface interface-name.unit-number;
    }
```

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), 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, 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, 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.
- 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 779](#)
- [Gateway Traceoptions Configuration Statements on page 792](#)

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>] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| 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 | <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] Hierarchy Level on page 456• show unified-edge ggsn-pgw call-rate statistics on page 1014 |

family (Mobile Interface)

| | |
|---------------------------------|---|
| Syntax | <code>family <i>family-name</i> {...}</code> |
| Hierarchy Level | <code>[edit interfaces <i>interface-name</i> unit <i>interface-unit-number</i>]</code> |
| 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 94• unit (Mobile Interface) on page 791 |

filter (Mobile Interface)

| | |
|---------------------------------|--|
| Syntax | <pre>filter { input <i>input-filter</i>; output <i>output-filter</i>; }</pre> |
| Hierarchy Level | <code>[edit interfaces <i>interface-name</i> unit <i>interface-unit-number</i>]</code> |
| 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 94• unit (Mobile Interface) on page 791 |

forwarding-packages

| | |
|---------------------------------|---|
| Syntax | <pre>forwarding-packages { mobility { ggsn-pgw; } }</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> <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 DPCs or MPCs for User Mobility Traffic on page 42 • Example: Configuring the MobileNext Broadband Gateway Chassis on page 43 |

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] Hierarchy Level on page 456• Configuring Broadband Gateway Home PLMNs and Gateways on page 10 |

history (Call-Rate Statistics)

| | |
|---------------------------------|---|
| Syntax | <code>history history;</code> |
| Hierarchy Level | [edit unified-edge gateways ggsn-pgw gateway-name call-rate-statistics] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| 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 should be 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 779• show unified-edge ggsn-pgw call-rate statistics on page 1014 |

home-plmn

| | |
|---------------------------------|--|
| Syntax | <pre>home-plmn { mcc [mcc] { mnc [mnc]; } }</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 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).</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 Broadband Gateway Home PLMNs and Gateways on page 10 • ggsn-pgw on page 782 |

input (Mobile Interface)

| | |
|---------------------------------|---|
| Syntax | input <i>input-filter</i> ; |
| 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 | <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 94 • filter (Mobile Interface) on page 780 |

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 96 |

interfaces (Mobile Interface)

| | |
|---------------------------------|---|
| Syntax | <pre> interfaces mif { description <i>description</i>; disable; mtu <i>mtu-size</i>; multi-chassis-protection { ... } no-traps; traceoptions { ... } 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] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | <p>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.</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 Mobile Interfaces for APNs on page 94 |

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] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | Configure the interval for which the call-rate statistics are calculated by the broadband gateway. |
| Options | interval —Interval, in minutes, for which the call-rate statistics should be 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 779• show unified-edge ggsn-pgw call-rate statistics on page 1014 |

mcc

Syntax `mcc [mcc] {
 mnc [mnc];
 }`

Hierarchy Level [edit unified-edge gateways ggsn-pgw *gateway-name* home-plmn]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

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.

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 10](#)
 • [home-plmn on page 783](#)

mnc

| | |
|--|---|
| Syntax | <code>mnc [mnc];</code> |
| Hierarchy Level | [edit unified-edge gateways ggsn-pgw <i>gateway-name</i> home-plmn mcc] |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| 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. |
| Options | <p><i>mnc</i>—Mobile network code.</p> <p>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.</p> |
| <div> NOTE: The MCC/MNC combination 00101 is reserved for test networks.</div> | |
| 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 | <ul style="list-style-type: none">• Configuring Broadband Gateway Home PLMNs and Gateways on page 10• mcc on page 787 |

mobility

| | |
|---------------------------------|---|
| Syntax | <pre>mobility { ggsn-pgw; }</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. |
| 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: You must include every Packet Forwarding Engine configured with the <code>ggsn-pgw</code> forwarding package at the [edit unified-edge gateways <code>ggsn-pgw gateway-name</code> 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.</p> </div> |
| Options | <code>ggsn-pgw</code> —Configure the router as a gateway GPRS support node (GGSN) or as a Packet Data Network Gateway (P-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 Interface DPCs or MPCs for User Mobility Traffic on page 42 Example: Configuring the MobileNext Broadband Gateway Chassis on page 43 forwarding-packages on page 781 |

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 94• interfaces (Mobile Interface) on page 785 |

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 94• filter (Mobile Interface) on page 780 |

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 94• interfaces (Mobile Interface) on page 785 |

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 18](#)
- [resource-management \(MobileNext Broadband Gateway\) on page 794](#)

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 452 • Configuring Mobile Options Trace Options on page 16 |

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 452](#)
 • [Configuring Resource Manager Trace Options on page 18](#)

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 18](#)
- [resource-management \(MobileNext Broadband Gateway\) on page 794](#)

traceoptions (MobileNext Broadband Gateway)

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 gateways ggsn-pgw *gateway-name*]

Release Information Statement introduced in Junos OS Mobility Release 11.2W.

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 **file *filename***—Name of the file that receives the output of the tracing operation. All files are placed in the `/var/log` directory.

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***—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can use one of the following flags:
 - **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 Level | interface—To view this statement in the configuration. |
| | interface-control—To add this statement to the configuration. |
| Related Documentation | • [edit unified-edge gateways] Hierarchy Level on page 456 |
| | • Configuring General Gateway Trace Options on page 14 |

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 /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">• 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 | • Configuring Mobile Options Trace Options on page 16 |
| | • mobile-options on page 793 |

tracoptions (Resource Management Client)

Syntax tracoptions {
 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 792](#)
 - [Configuring Resource Manager Trace Options on page 18](#)

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(RMPD) 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 18• server (Resource Management) on page 795 |

PART 12

Command Reference

- [AAA Operational Commands on page 809](#)
- [Anchor Packet Forwarding Engine Redundancy and Aggregated Multiservices High Availability Operational Commands on page 833](#)
- [APN and Related Operational Commands on page 845](#)
- [Charging Operational Commands on page 875](#)
- [Class of Service \(CoS\) Operational Commands on page 957](#)
- [Exception Handling Operational Commands on page 963](#)
- [GPRS Tunneling Protocol \(GTP\) Operational Commands on page 973](#)
- [Service Applications Operational Commands on page 981](#)
- [System Architecture Operational Commands on page 1013](#)

CHAPTER 29

AAA Operational Commands

clear unified-edge ggsn-pgw aaa radius statistics

| | |
|---------------------------------|---|
| Syntax | clear unified-edge ggsn-pgw aaa radius statistics (authentication accounting dynamic-requests all) [name <i>name</i>] [fpc-slot <i>fpc</i> pic-slot <i>pic</i>] |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Clear statistics for the AAA RADIUS server. |
| Options | <p>authentication accounting dynamic-requests all—Clear statistics for the specified parameter.</p> <p>fpc-slot <i>fpc</i> pic-slot <i>pic</i>—Clear statistics for the services PIC in the specified FPC and PIC slots.</p> <p>name <i>name</i>—Clear statistics for the specified server.</p> |
| Required Privilege Level | clear |
| Related Documentation | <ul style="list-style-type: none">• show unified-edge ggsn-pgw aaa radius statistics on page 817 |

clear unified-edge ggsn-pgw aaa statistics

| | |
|---------------------------------|--|
| Syntax | clear unified-edge ggsn-pgw aaa statistics accounting (authentication accounting dynamic-requests all) [<i>fpc-slot fpc</i> <i>pic-slot pic</i>] |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Clear global statistics related to authentication, accounting, dynamic requests, or all of them on the gateway. |
| Options | <i>fpc-slot fpc</i> <i>pic-slot pic</i> —Clear accounting statistics for the services PIC in the specified FPC and PIC slots. |
| Required Privilege Level | clear |
| Related Documentation | <ul style="list-style-type: none">• show unified-edge ggsn-pgw aaa statistics authentication on page 821• show unified-edge ggsn-pgw aaa statistics accounting on page 819• show unified-edge ggsn-pgw aaa statistics dynamic-requests on page 823 |

clear unified-edge ggsn-pgw address-assignment pool-name

| | |
|---------------------------------|---|
| Syntax | clear unified-edge ggsn-pgw address-assignment pool-name <i>pool-name</i> |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Clear the sessions that have been assigned addresses from this pool. |
| Options | pool-name <i>pool-name</i> —Pool name for the address assignment. |
| Required Privilege Level | clear |
| Related Documentation | <ul style="list-style-type: none">• show unified-edge ggsn-pgw address-assignment pool name on page 827 |

Sample Output

| | |
|---|---|
| clear unified-edge ggsn-pgw address-assignment pool name | user@host> clear unified-edge ggsn-pgw address-assignment pool name Initiated clearing of sessions in the pool |
|---|---|

clear unified-edge ggsn-pgw address-assignment statistics

| | |
|---------------------------------|--|
| Syntax | clear unified-edge ggsn-pgw address-assignment statistics [<i>fpc-slot fpc</i> <i>pic-slot pic</i>] |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Clear global address assignment statistics on the gateway. |
| Options | <i>fpc-slot fpc</i> <i>pic-slot pic</i> —Clear statistics for the services PIC in the specified FPC and PIC slots. |
| Required Privilege Level | clear |
| Related Documentation | <ul style="list-style-type: none">• show unified-edge ggsn-pgw address-assignment statistics on page 831 |

show unified-edge ggsn-pgw aaa network element-group status

| | |
|---------------------------------|---|
| Syntax | show unified-edge ggsn-pgw aaa network element-group status [name <i>ne-grp-name</i>] [fpc-slot <i>fpc</i> pic-slot <i>pic</i>] |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Display the AAA network element group status. |
| Options | <p>fpc-slot <i>fpc</i> pic-slot <i>pic</i>—Display the status of the services PIC in the specified FPC and PIC slots.</p> <p>name <i>ne-grp-name</i>—Display the status of the specified network element group. If the name of the group is not specified, then display status of all the network element groups.</p> |
| Required Privilege Level | view |
| Output Fields | Table 46 on page 814 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 46: 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 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. |
| Members | Members of the network element group and their mandatory status in the group. |

Sample Output

```

show unified-edge ggsn-pgw aaa network element-group status
user@host> show unified-edge ggsn-pgw aaa network element-group status

network element-group: NEG_1
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 ggsn-pgw aaa network element-group status name NEG_1
user@host> show unified-edge ggsn-pgw aaa network element-group status name NEG_1

network element-group: NEG_1
Broadcast: Disabled
Members:
  ne1, Mandatory: No
  ne2, Mandatory: No

show unified-edge ggsn-pgw aaa network element-group status name ne_group1
user@host> show unified-edge ggsn-pgw aaa network element-group status name ne_group1

network element-group: ne_group1
Broadcast: Enabled
Members:
  ne1, Mandatory: No
  ne2, Mandatory: Yes
```

show unified-edge ggsn-pgw aaa network element status

| | |
|---------------------------------|---|
| Syntax | show unified-edge ggsn-pgw aaa network element status [name <i>ne-name</i>] [fpc-slot <i>fpc</i> pic-slot <i>pic</i>] |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Display the AAA network element status. |
| Options | <p>fpc-slot <i>fpc</i> pic-slot <i>pic</i>—Display the status of the services PIC in the specified FPC and PIC slots.</p> <p>name <i>ne-name</i>—Display the status of the specified network element. If the name of the network element is not specified, then display status of all the network elements.</p> |
| Required Privilege Level | view |
| Output Fields | Table 47 on page 816 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. |

Table 47: 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. |
| 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. |
| State | State of the RADIUS server whether 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: ne1 (FPC/PIC: 0/0)
  Server: mobdevlinux1, Priority: 1, State: Active

Network-element: ne2 (FPC/PIC: 0/0)
  Server: vm-moblinux3, Priority: 1, State: Active

```


show unified-edge ggsn-pgw aaa radius statistics

| | |
|---------------------------------|--|
| Syntax | show unified-edge ggsn-pgw aaa radius statistics (authentication accounting dynamic-requests) [name <i>server-name</i>] [fpc-slot <i>fpc</i> pic-slot <i>pic</i>] |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Display the statistics for the AAA RADIUS server. |
| Options | <p>authentication accounting dynamic-requests—Display statistics for the specified parameter.</p> <p>fpc-slot <i>fpc</i> pic-slot <i>pic</i>—Display statistics for the services PIC in the specified FPC and PIC slots.</p> <p>name <i>server-name</i> —Display statistics for the specified RADIUS server name. If the RADIUS server name is not specified, display statistics for all configured servers.</p> |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> • clear unified-edge ggsn-pgw aaa radius statistics on page 810 |
| Output Fields | Table 48 on page 817 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 48: show unified-edge ggsn-pgw aaa radius statistics Output Fields

| Field Name | Field Description |
|-------------------|---|
| RADIUS server | Name of the RADIUS server. |
| Port | Port number of the RADIUS server. |
| FPC/PIC | FPC and PIC slot numbers. |
| State | State of the RADIUS server whether dead or alive. |
| Duration | Duration in HH:MM:SS format for which the RADIUS server is active. |
| Previous duration | Duration in HH:MM:SS format for which the RADIUS server was active. |
| Flaps | Number of times the RADIUS server transitioned from the active to dead state. |
| Requests | Number of requests sent to the RADIUS server from the FPC slot and PIC slot. |
| Responses | Number of responses received from the RADIUS server on the FPC slot and PIC slot. |

Sample Output

```
show unified-edge ggsn-pgw aaa radius statistics authentication
user@host> show unified-edge ggsn-pgw aaa radius statistics authentication

RADIUS server: radius1
Address: 50.50.50.101 Port: 1812
FPC/
PIC  State      Duration      Previous
0/0  Active      01:37:10      00:00:00      0      1      1

RADIUS server: radius2
Address: 50.50.50.100 Port: 1812
FPC/
PIC  State      Duration      Previous
0/0  Active      01:37:10      00:00:00      0      0      0
```

show unified-edge ggsn-pgw aaa statistics accounting

| | |
|---------------------------------|--|
| Syntax | show unified-edge ggsn-pgw aaa statistics accounting [<i>fpc-slot fpc</i> <i>pic-slot pic</i>] |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Display the accounting statistics at the chassis or box level. |
| Options | <i>fpc-slot fpc</i> <i>pic-slot pic</i> —Display the accounting statistics for the services PIC in the specified FPC and PIC slots. |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> clear unified-edge ggsn-pgw aaa statistics on page 811 |
| Output Fields | Table 49 on page 819 lists the output fields for the show unified-edge ggsn-pgw aaa statistics accounting command. Output fields are listed in the approximate order in which they appear. |

Table 49: show unified-edge ggsn-pgw aaa statistics accounting Output Fields

| Field Name | Field Description |
|--------------------|--|
| Pending requests | Number of requests pending in the queue to be sent to the RADIUS server. |
| Requests | Total number of accounting-request packets sent to a RADIUS server. |
| Requests timed out | Number of requests that were timed out and did not receive a response from the RADIUS server. |
| Response errors | Number of errors occurred on the gateway while accounting-request packets process the response from the RADIUS server. |
| Responses Success | Number of accounting-response success packets received from the RADIUS server. |
| Transmit errors | Number of errors occurred on the gateway while accounting-request packets are transmitted to the RADIUS server. |

Sample Output

```

show unified-edge user@host> show unified-edge ggsn-pgw aaa statistics accounting
ggsn-pgw aaa
statistics accounting
Accounting module statistics
Requests:          3
Responses Success: 2
Requests timed out: 0
Transmit errors:   0

```

Response errors: 0
Pending requests: 0

show unified-edge ggsn-pgw aaa statistics authentication

| | |
|---------------------------------|--|
| Syntax | show unified-edge ggsn-pgw aaa statistics authentication [<i>fpc-slot fpc</i> <i>pic-slot pic</i>] |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Display the authentication statistics at the chassis or box level. |
| Options | <i>fpc-slot fpc</i> <i>pic-slot pic</i> —Display the authentication statistics for the services PIC in the specified FPC and PIC slots. |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> • clear unified-edge ggsn-pgw aaa statistics on page 811 |
| Output Fields | Table 50 on page 821 lists the output fields for the show unified-edge ggsn-pgw aaa statistics authentication command. Output fields are listed in the approximate order in which they appear. |

Table 50: show unified-edge ggsn-pgw aaa statistics authentication Output Fields

| Field Name | Field Description |
|--------------------|--|
| Accepts | Number of access-accept responses received from the RADIUS server. |
| Challenges | Number of access-challenge responses received from the RADIUS server. |
| Pending requests | Number of requests pending in the queue to be sent to the RADIUS server. |
| Rejects | Number of access-reject responses received from the RADIUS server. |
| Requests | Total number of authentication requests sent to the RADIUS server. |
| Requests timed out | Number of requests that did not receive a response from the RADIUS server. |
| Response errors | Number of errors occurred on the gateway while authentication-request packets process the response from the RADIUS server. |
| Transmit errors | Number of errors occurred on the gateway while authentication-request packets are transmitted to the RADIUS server. |

Sample Output

```

show unified-edge ggsn-pgw aaa statistics authentication
user@host> show unified-edge ggsn-pgw aaa statistics authentication
Authentication module statistics
Requests:          1
Accepts:           1
Rejects:           0

```

Challenges: 0
Requests timed out: 0
Transmit errors: 0
Response errors: 0
Pending requests: 0

show unified-edge ggsn-pgw aaa statistics dynamic-requests

| | |
|---------------------------------|--|
| Syntax | show unified-edge ggsn-pgw aaa statistics dynamic-requests [<i>fpc-slot fpc</i> <i>pic-slot pic</i>] |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Display dynamic-requests statistics at the chassis or box level. |
| Options | <i>fpc-slot fpc</i> <i>pic-slot pic</i> —Display dynamic-requests statistics for the services PIC in the specified FPC and PIC slots. |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> clear unified-edge ggsn-pgw aaa statistics on page 811 |
| Output Fields | Table 51 on page 823 lists the output fields for the show unified-edge ggsn-pgw aaa statistics dynamic-requests command. Output fields are listed in the approximate order in which they appear. |

Table 51: show unified-edge ggsn-pgw aaa statistics dynamic-requests Output Fields

| Field Name | Field Description |
|-----------------------|--|
| CoA Acks sent | Number of change of authorization (COA) acknowledgements sent to RADIUS clients. |
| CoA Nacks sent | Number of change of authorization (COA) Nacks sent to RADIUS clients. |
| CoA Requests received | Number of change of authorization (COA) requests received from RADIUS clients. |
| Dm Acks sent | Number of DM acknowledgements sent to RADIUS clients. |
| Dm Nacks sent | Number of DM Nacks sent to RADIUS clients. |
| Dm Requests received | Number of DM requests received from RADIUS clients. |
| Dropped | Number of dynamic requests dropped. |
| Requests received | Total number of dynamic requests received from RADIUS clients. |

Sample Output

```

show unified-edge ggsn-pgw aaa statistics dynamic-requests
user@host> show unified-edge ggsn-pgw aaa statistics dynamic-requests
Dynamic Requests module statistics
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 ggsn-pgw address-assignment group

| | |
|---------------------------------|--|
| Syntax | show unified-edge ggsn-pgw address-assignment statistics brief detail name <i>group-name</i> routing-instance <i>routing-instance-name</i> fpc-slot <i>slot-number</i> pic-slot <i>slot-number</i> |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Display information about an address assignment group at the chassis or box level. |
| Options | <p>brief detail—(Optional) Display the specified level of output.</p> <p>fpc-slot <i>slot-number</i> pic-slot <i>slot-number</i>—(Optional) Display statistics about the services PIC in the specified FPC and PIC slots.</p> <p>name <i>group-name</i>—Display information about the specified group.</p> <p>routing-instance <i>routing instance name</i>—(Optional) Display information about 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> |
| Output Fields | Table 52 on page 825 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. |

Table 52: show unified-edge ggsn-pgw address-assignment-group Output Fields

| Field Name | Field Description |
|-------------------------|---|
| Group | Name of the address-assignment group. |
| Total addresses | Total number of addresses available in the group. |
| Addresses in use | Number of addresses in the group that are currently in use. |
| Address usage (percent) | Percentage utilization of the total addresses. |
| Routing instance | Routing instance to which the group belongs. |
| Pool information | Information about the pools belonging to this group. |

Sample Output

```

show unified-edge ggsn-pgw address-assignment group detail
user@host> show unified-edge ggsn-pgw address-assignment group detail
Group: g1
  Total addresses:      512
  Addresses in use:     0
  Address usage (percent): 0
  Routing instance:     default
  Pool information:

```

| Name | Total | In-use | Util (%) |
|------|-------|--------|-------------|
| p1 | 256 | 0 | 0 |
| p2 | 256 | 0 | 0 |

show unified-edge ggsn-pgw address-assignment pool name

| | |
|---------------------------------|---|
| Syntax | show unified-edge ggsn-pgw address-assignment pool name <i>poolname</i> [fpc-slot <i>fpc</i> pic-slot <i>pic</i>] <(ranges range <i>rangename</i>)> |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Display information for a specific pool at the chassis or box level. |
| Options | <p>fpc-slot <i>fpc</i> pic-slot <i>pic</i>—Display information for the services PIC in the specified FPC and PIC slots.</p> <p>pool name <i>poolname</i>—(Optional) Display information for the specified pool. If the pool name is not specified, display information for all pools.</p> <p>ranges range <i>rangename</i>—(Optional) Display information for all the ranges or for a particular range in the specified pool.</p> |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> • clear unified-edge ggsn-pgw address-assignment pool-name on page 812 |
| Output Fields | Table 53 on page 827 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 53: show unified-edge ggsn-pgw address-assignment pool Output Fields

| Field Name | Field Description |
|---------------------------|---|
| Addresses in aging period | Number of addresses in the aging period. |
| Addresses in use | Number of addresses that have been allocated. |
| Addresses skipped | Number of addresses that are skipped from allocation. |
| Address usage (percent) | Percentage utilization of the total addresses. |
| Pool name | Name of the address-assignment pool. |
| Routing instance | Name of the routing instance to which the pool belongs. |
| Total addresses | Total number of addresses available in the pool. |

Sample Output

```
show unified-edge user@host> show unified-edge ggsn-pgw address-assignment pool
ggsn-pgw
address-assignment Pool: <name>
pool              Total addresses:      65278
                  Addresses in use:      1
                  Addresses skipped:      80
                  Address usage (percent): 0
                  Addresses in aging period: 0
                  Routing instance:      default
```

show unified-edge ggsn-pgw address-assignment service-mode

| | |
|---------------------------------|--|
| Syntax | show unified-edge ggsn-pgw address-assignment service-mode <brief detail> <pool <i>pool-name</i> > <routing-instance <i>routing-instance-name</i> > |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Display service mode information about the address assignment. |
| Options | brief detail—(Optional) Display the specified level of output. pool <i>pool-name</i> —(Optional) Display service mode information about the specified pool. routing-instance <i>routing-instance-name</i> —(Optional) Display service mode information about the specified routing instance. |
| Required Privilege Level | view |
| List of Sample Output | show unified-edge ggsn-pgw address-assignment service-mode on page 829 |
| Output Fields | Table 54 on page 829 lists the output fields for the show unified-edge ggsn-pgw address-assignment service-mode command. Output fields are listed in the approximate order in which they appear. |

Table 54: show unified-edge ggsn-pgw address-assignment service-mode Output Fields

| Field Name | Field Description |
|------------------|---|
| Pool Name | Name of the pool. |
| Routing Instance | Name of the routing instance to which the pool belongs. |
| Service Mode | Service mode for the address assignment. The following service modes are possible: <ul style="list-style-type: none"> • Operational—Address assignment is in operational mode. • Maintenance—Address assignment is in maintenance mode. |

Sample Output

```

show unified-edge user@host> show unified-edge ggsn-pgw address-assignment service-mode
ggsn-pgw          Maintenance Mode
address-assignment MM Active Phase - System is ready to accept configuration changes for all
service-mode      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

```

Gi-VR
default

jnpr-Gi
abc2

Operational
Operational

show unified-edge ggsn-pgw address-assignment statistics

| | |
|---------------------------------|--|
| Syntax | show unified-edge ggsn-pgw address-assignment statistics [<i>fpc-slot fpc</i> <i>pic-slot pic</i>] |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Display statistics for an address assignment at the chassis or box level. |
| Options | <i>fpc-slot fpc</i> <i>pic-slot pic</i> —Display statistics for the services PIC in the specified FPC and PIC slots. |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> • clear unified-edge ggsn-pgw address-assignment statistics on page 813 |
| Output Fields | Table 55 on page 831 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 55: show unified-edge ggsn-pgw address-assignment statistics Output Fields

| Field Name | Field Description |
|---------------------------|---|
| Total address allocations | Total number of addresses allocated. |
| Total address releases | Total number of addresses released. |
| Total allocation failures | Total number of address allocations failed. |

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: 0
Total allocation failures: 0
Total address releases: 0

```


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 835 |
| List of Sample Output | request interface load-balancing revert mams-4/0/0 (Aggregated Multiservices) on page 834 |
| 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 834 |
| List of Sample Output | request interface load-balancing switchover force mams-4/0/0 (Aggregated Multiservices) on page 835 |
| 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 842](#)

List of Sample Output [show interfaces anchor-group brief on page 837](#)
[show interfaces anchor-group detail on page 838](#)

Output Fields [Table 56 on page 836](#) lists the output fields for the `show interfaces anchor-group` command. Output fields are listed in the approximate order in which they appear.

Table 56: 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 56: 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 842 |
| List of Sample Output | show interfaces load-balancing on page 840 show interfaces load-balancing detail on page 840 show interfaces load-balancing ams0 detail on page 841 |
| Output Fields | Table 57 on page 839 lists the output fields for the show interfaces load-balancing command. Output fields are listed in the approximate order in which they appear. |

Table 57: 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 57: 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 unified-edge ggsn-pgw system interfaces

| | |
|---------------------------------|---|
| Syntax | show unified-edge ggsn-pgw system interfaces |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Display information about the aggregated Packet Forwarding Engine and the aggregated multiservices (AMS) interfaces and their states on the broadband gateway. |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> • show interfaces anchor-group (Aggregated Packet Forwarding Engine) on page 836 • show interfaces load-balancing (Aggregated Multiservices) on page 839 |
| List of Sample Output | show unified-edge ggsn-pgw system interfaces on page 843 |
| Output Fields | Table 58 on page 842 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 58: show unified-edge ggsn-pgw system interfaces

| Field Name | Field Description |
|--------------------------|--|
| Gateway | Name of the broadband gateway. The internal ID, which is currently not supported, corresponding to the gateway is displayed. |
| Interfaces | Name of the interface. This can be one of the following interfaces: <ul style="list-style-type: none"> • Aggregated multiservices (ams). • Aggregated Packet Forwarding Engine (apfe). • Member of aggregated multiservices (mams-). • Multiservices (ms-). • Packet Forwarding Engine (pfe-). |
| Members | For ams and apfe interfaces, the member interfaces that are a part of the aggregated interfaces is displayed. |
| Operational State | Indicates whether the interface is operational (Active) or not operational (Inactive). |
| Redundancy Role | Redundancy state in which the interface was configured. <ul style="list-style-type: none"> • Primary: Indicates that the interface is a primary member. • Secondary: Indicates that the interface is a backup to all the primary members. • Standalone: Indicates that 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 Interface Status Legend:
interfaces
Active   : Operational      Inactive  : Non-Operational
MM       : Service mode maintenance

Gateway: PGW (1)



| Interfaces | Members     | Operational State | Redundancy Role |
|------------|-------------|-------------------|-----------------|
| ams0       | mams-2/0/0  | Active            | Primary         |
|            | mams-11/1/0 | Active            | Secondary       |
| ams1       | mams-2/1/0  | Active            | Primary         |
|            | mams-11/0/0 | Active            | Secondary       |
| ams2       | mams-3/0/0  | Active            | Primary         |
|            | mams-4/0/0  | Active            | Secondary       |
| ams3       | mams-3/1/0  | Active            | Primary         |
|            | mams-4/1/0  | Active            | Secondary       |
| apfe0      | pfe-0/0/0   | Active            | Primary         |
|            | pfe-1/0/0   | Active            | Secondary       |
|            | pfe-0/2/0   | Active            | Primary         |
|            | pfe-1/2/0   | Active            | Secondary       |
| pfe-5/0/0  |             | Active            | Standalone      |
| pfe-5/2/0  |             | Active            | Standalone      |
| pfe-7/0/0  |             | Active            | Standalone      |
| pfe-7/2/0  |             | Active            | Standalone      |


```


CHAPTER 31

APN and Related Operational Commands

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 broadband gateway. If an access point name (APN) is specified, then only the statistics for that APN are cleared. |
| Options | <code>gateway <i>gateway</i></code> —Clear the statistics for the specified broadband gateway. <code>apn <i>apn</i></code> —(Optional) Clear the statistics for the specified APN. |
| Required Privilege Level | clear |
| Related Documentation | <ul style="list-style-type: none">• show unified-edge ggsn-pgw statistics on page 860 |
| List of Sample Output | clear unified-edge ggsn-pgw statistics gateway pgw on page 846 clear unified-edge ggsn-pgw statistics gateway pgw apn apn-1 on page 846 |
| 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 statistics gateway pgw</code> | <code>user@host> clear unified-edge ggsn-pgw statistics gateway pgw</code> |
| <code>clear unified-edge ggsn-pgw statistics gateway pgw apn apn-1</code> | <code>user@host> clear unified-edge ggsn-pgw statistics gateway pgw apn apn-1</code> |

clear unified-edge ggsn-pgw subscribers

| | |
|---------------------------------|---|
| Syntax | 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> > |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Clear the subscribers for the broadband gateway based on the options specified. |
| Options | <p>gateway <i>gateway</i>—Clear the subscribers for the specified broadband gateway.</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 849 • clear unified-edge ggsn-pgw subscribers peer on page 850 • show unified-edge ggsn-pgw subscribers on page 865 |
| List of Sample Output | clear unified-edge ggsn-pgw subscribers gateway pgw on page 847 clear unified-edge ggsn-pgw subscribers gateway pgw apn apn-1 on page 848 |
| Output Fields | When you enter this command, you are provided feedback on the status of your request. |

Sample Output

```
clear unified-edge ggsn-pgw subscribers
gateway pgw
```

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

```
clear unified-edge ggsn-pgw subscribers gateway pgw apn apn-1
user@host> clear unified-edge ggsn-pgw subscribers gateway pgw apn apn-1
```


clear unified-edge ggsn-pgw subscribers charging

| | |
|---------------------------------|---|
| Syntax | clear unified-edge ggsn-pgw subscribers charging gateway <i>gateway</i> <charging-profile <i>charging-profile</i> > <transport-profile <i>transport-profile</i> > |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Clear the charging information for subscribers on the broadband gateway based on the options specified. |
| Options | <p>gateway <i>gateway</i>—Clear the charging information for all subscribers for the specified gateway name.</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> |
| Required Privilege Level | clear |
| Related Documentation | <ul style="list-style-type: none"> • clear unified-edge ggsn-pgw subscribers on page 847 • clear unified-edge ggsn-pgw subscribers peer on page 850 • show unified-edge ggsn-pgw subscribers on page 865 |
| List of Sample Output | clear unified-edge ggsn-pgw subscribers charging gateway pgw on page 849 |
| Output Fields | When you enter this command, you are provided feedback on the status of your request. |

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 | <code>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>></code> |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Clear the information for subscribers anchored for the specified GPRS tunneling protocol (GTP) peer. The GTP peer can be a serving GPRS support node (SGSN) or a Serving Gateway (S-GW). |
| Options | <p><code>gateway <i>gateway</i></code>—Clear the subscribers for the specified gateway name.</p> <p><code>remote-addr <i>remote-addr</i></code>—Clear the information for subscribers anchored on the peer with the specified IPv4 address.</p> <p><code>local-addr <i>local-addr</i></code>—(Optional) Clear the subscriber matching the specified local IPv4 address of the broadband gateway on that interface.</p> <p><code>routing-instance <i>routing-instance</i></code>—(Optional) Clear the subscriber matching the specified routing instance. Each instance corresponds to a VRF on the interface.</p> |
| Required Privilege Level | clear |
| Related Documentation | <ul style="list-style-type: none">• clear unified-edge ggsn-pgw subscribers on page 847• clear unified-edge ggsn-pgw subscribers charging on page 849• show unified-edge ggsn-pgw subscribers on page 865 |
| List of Sample Output | clear unified-edge ggsn-pgw subscribers peer gateway pgw remote-addr 11.11.11.2 local-addr 123.1.1.1 on page 850 |
| 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 subscribers peer gateway pgw remote-addr 11.11.11.2 local-addr 123.1.1.1</code> | <code>user@host> clear unified-edge ggsn-pgw subscribers peer gateway pgw remote-addr 11.11.11.2 local-addr 123.1.1.1</code> |
|---|---|

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) in the broadband gateway. If an APN is not specified, then the information for all APNs in the broadband gateway 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 gateway name.</p> |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> • show unified-edge ggsn-pgw gateway service-mode on page 858 |
| List of Sample Output | show unified-edge ggsn-pgw apn service-mode brief on page 852 show unified-edge ggsn-pgw apn service-mode detail on page 852 show unified-edge ggsn-pgw apn service-mode apn-name apnv4-lp-vrf1-02 on page 853 |
| Output Fields | Table 59 on page 851 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 59: show unified-edge ggsn-pgw apn service-mode Output Fields

| Field Name | Field Description |
|--------------|---|
| APN Name | Name of the APN. |
| Service Mode | <p>Service mode for the APN. The following service modes are possible:</p> <ul style="list-style-type: none"> • Operational—The APN is in operational mode. • Maintenance—The 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 |
| apnv4-gp-dvrf-02 | Operational |
| apnv4-gp-dvrf-03 | Operational |
| apnv4-gp-dvrf-04 | Operational |
| apnv4-gp-vrf1-01 | Operational |
| apnv4-gp-vrf1-02 | Operational |
| apnv4-gp-vrf1-03 | 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

APN Name      : apnv4-gp-dvrf-02
Service Mode  : Operational

APN Name      : apnv4-gp-dvrf-03
Service Mode  : Operational

APN Name      : apnv4-gp-dvrf-04
Service Mode  : Operational

APN Name      : apnv4-gp-vrf1-01
Service Mode  : Operational

APN Name      : apnv4-gp-vrf1-02
Service Mode  : Operational

APN Name      : apnv4-gp-vrf1-03
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
                  attributes of this object and its sub-hierarchies.
apn-name          MM In/Out Phase - System is ready to accept configuration changes only for
apnv4-lp-vrf1-02 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 | <code>show unified-edge ggsn-pgw apn statistics apn-name <i>apn-name</i></code> <code><gateway <i>gateway</i>></code> |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Display the statistics for an access point name (APN) in the broadband gateway. |
| Options | <code>apn-name <i>apn-name</i></code> —Name of the APN for which you want the statistics displayed. <code>gateway <i>gateway</i></code> —(Optional) Name of the broadband gateway to which the APN belongs. |
| Required Privilege Level | view |
| List of Sample Output | show unified-edge ggsn-pgw apn statistics apn-name apn-1 on page 856 |
| Output Fields | Table 60 on page 854 lists the output fields for the <code>show unified-edge ggsn-pgw apn statistics</code> command. Output fields are listed in the approximate order in which they appear. |

Table 60: show unified-edge ggsn-pgw apn statistics Output Fields

| Field Name | Field Description |
|---|---|
| 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. |
| 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). |

Table 60: show unified-edge ggsn-pgw apn statistics Output Fields (*continued*)

| Field Name | Field Description |
|---|--|
| 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 gateway GPRS support node (GGSN) or the Packet Data Network Gateway (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. |
| Session Establishments Failed (by GTP cause) | <p>Number of session establishments that failed, listed according to the following GTP cause codes (returned in the GTP Response message):</p> <ul style="list-style-type: none"> • Others • Service unavailable • System failure • No resources • No address • Service denied • Authentication Fail • APN access denied |
| Miscellaneous Packet Statistics | |
| IPv6 Router Solicitations received | Number of IPv6 router solicitations received by the APN on the broadband gateway. |

Table 60: show unified-edge ggsn-pgw apn statistics Output Fields (continued)

| Field Name | Field Description |
|---|---|
| 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. |
| 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 user@host> show unified-edge ggsn-pgw apn statistics apn-name apn-1
ggsn-pgw apn      Control plane APN statistics:
statistics apn-name Session establishment attempts:           3
apn-1              Successful session establishments:           3
                   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:         3
    dynamic IP allocation success:          3
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:     5
    IPv6 Router Advertisement transmitted:  14
    IPv6 Neighbor Solicitations received:    15
    IPv6 Neighbor Advertisement transmitted: 15
Data plane GTP statistics (Gn/S5/S8):
    Input   packets:      20
    Input   bytes:       1200
    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:       1200
    Discarded packets:    0

```

show unified-edge ggsn-pgw gateway service-mode

| | |
|---------------------------------|---|
| Syntax | <code>show unified-edge ggsn-pgw gateway service-mode</code> <code><brief detail></code> <code><gateway-name gateway-name></code> |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Display service mode information for the broadband gateway. |
| Options | <p><code>none</code>—(Same as <code>brief</code>) Display the gateway service mode information in brief.</p> <p><code>brief detail</code> —(Optional) Display the specified level of output.</p> <p><code>gateway-name gateway-name</code>—(Optional) Display service mode information for the specified gateway.</p> |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> show unified-edge ggsn-pgw apn service-mode on page 851 |
| List of Sample Output | show unified-edge ggsn-pgw gateway service-mode brief on page 858 show unified-edge ggsn-pgw gateway service-mode detail on page 859 show unified-edge ggsn-pgw gateway service-mode gateway-name pgw on page 859 |
| Output Fields | Table 61 on page 858 lists the output fields for the <code>show unified-edge ggsn-pgw gateway service-mode</code> command. Output fields are listed in the approximate order in which they appear. |

Table 61: show unified-edge ggsn-pgw gateway service-mode Output Fields

| Field Name | Field Description |
|--------------|--|
| Gateway Name | Name of the broadband gateway. |
| 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. |

Sample Output

```

show unified-edge ggsn-pgw gateway service-mode brief
user@host> show unified-edge ggsn-pgw gateway 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

```


show unified-edge ggsn-pgw statistics

| | |
|---------------------------------|--|
| Syntax | <code>show unified-edge ggsn-pgw statistics</code> <code><gateway gateway></code> |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Display the statistics for the broadband gateway. |
| Options | <code>gateway gateway</code> —(Optional) Display the statistics for the specified gateway name. |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> clear unified-edge ggsn-pgw statistics on page 846 |
| List of Sample Output | show unified-edge ggsn-pgw statistics on page 861 |
| Output Fields | Table 62 on page 860 lists the output fields for the <code>show unified-edge ggsn-pgw statistics</code> command. Output fields are listed in the approximate order in which they appear. |

Table 62: show unified-edge ggsn-pgw statistics Output Fields

| Field Name | Field Description |
|---|---|
| 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. |
| Successful gateway initiated deactivations | Number of deactivations initiated by the broadband gateway that were successful. |
| Data Plane GTP Statistics (Gn/S5/S8) | |
| Input packets | Number of incoming GTP data packets on the Gn interface. |

Table 62: show unified-edge ggsn-pgw statistics Output Fields (*continued*)

| Field Name | Field Description |
|---------------------------------------|--|
| Input bytes | Number of octets of incoming GTP data packets on the Gn interface. |
| Output packets | Number of outgoing GTP data packets on the Gn interface. |
| Output bytes | Number of octets of outgoing GTP data packets on the Gn interface. |
| Discarded packets | Number of discarded GTP data packets on the Gn interface. |
| 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:      20
  Successful session establishments:    20
  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:      804
  Input   bytes:      73968
  Output  packets:      804
  Output  bytes:      73968
  Discarded packets:      0
Data plane GTP statistics (Gi):
  Input   packets:      804
  Input   bytes:      73968
  Output  packets:      804
  Output  bytes:      73968
  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 (eutan | gan | geran | hspa | others | utran | wlan)>`
 `<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 the broadband gateway.

Options none—(Same as brief) Display the gateway 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 gateway name.

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).

rat-type (eutan | gan | geran | hspa | others | utran | wlan)—(Optional) Display the status information for the specified Radio Access Technology (RAT).

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 960](#)

List of Sample Output [show unified-edge ggsn-pgw status on page 863](#)
[show unified-edge ggsn-pgw status detail on page 863](#)
[show unified-edge ggsn-pgw status detail fpc-slot 9 pic-slot 1 on page 864](#)

Output Fields [Table 63 on page 863](#) 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 63: show unified-edge ggsn-pgw status Output Fields

| Field Name | Field Description |
|--------------------|---|
| FPC SLOT | FPC slot number of the interface for which the status information is displayed. |
| PIC SLOT | PIC slot number of the FPC for which the status information is displayed. |
| Active Subscribers | Number of active subscribers. |
| Active Sessions | Number of active sessions. |
| Active Bearers | Number of active bearers or PDP contexts. |
| CPU Load (%) | Percentage of the CPU load. |
| Memory Load (%) | Percentage of the memory load. |

Sample Output

```

show unified-edge ggsn-pgw status    user@host> show unified-edge ggsn-pgw status
                                         Mobile gateway status:
                                         Active Subscribers   :           20
                                         Active Sessions       :           20
                                         Active Bearers        :           20
                                         CPU Load (%)          :            0
                                         Memory Load (%)       :           25

show unified-edge ggsn-pgw status detail user@host> show unified-edge ggsn-pgw status detail
                                         Mobile gateway status:

                                         FPC SLOT: 10 PIC SLOT: 0
                                         Active Subscribers   :            0
                                         Active Sessions       :            0
                                         Active Bearers        :            0
                                         CPU Load (%)          :            0
                                         Memory Load (%)       :           32
                                         Mobile gateway status:

```

```
FPC SLOT: 10 PIC SLOT: 1
Active Subscribers   :           0
Active Sessions      :           0
Active Bearers       :           0
CPU Load (%)         :           0
Memory Load (%)      :          44
Mobile gateway status:
```

```
FPC SLOT: 9 PIC SLOT: 1
Active Subscribers   :           0
Active Sessions      :           0
Active Bearers       :           0
CPU Load (%)         :           0
Memory Load (%)      :          33
```

```
show unified-edge user@host> show unified-edge ggsn-pgw status detail fpc-slot 9 pic-slot 1
ggsn-pgw status detail
fpc-slot 9 pic-slot 1
Mobile gateway status:

FPC SLOT: 9 PIC SLOT: 1
Active Subscribers   :           0
Active Sessions      :           0
Active Bearers       :           0
CPU Load (%)         :           0
Memory Load (%)      :          33
```


show unified-edge ggsn-pgw subscribers

Syntax show unified-edge ggsn-pgw subscribers
 <brief | 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*>
 <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.

Description Display the subscriber information for the broadband gateway.

Options none—(Same as brief) Display the subscriber information in brief.

brief | 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.

`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 847](#)
- [clear unified-edge ggsn-pgw subscribers charging on page 849](#)
- [clear unified-edge ggsn-pgw subscribers peer on page 850](#)

List of Sample Output

[show unified-edge ggsn-pgw subscribers on page 871](#)
[show unified-edge ggsn-pgw subscribers extensive on page 872](#)
[show unified-edge ggsn-pgw subscribers fpc-slot 7 pic-slot 0 on page 873](#)

Output Fields

[Table 64 on page 866](#) 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 64: show unified-edge ggsn-pgw subscribers Output Fields

| Field Name | Field Description | Level of Output |
|--------------------|--|-----------------|
| IMSI | IMSI of the subscriber's user equipment. | brief |
| MSISDN | MSISDN number of the subscriber's user equipment. | brief |
| Subscriber Address | IP address of the subscriber's user equipment. | brief |
| Peer Address | IP address of the GTP peer through which the subscriber is connected to the broadband gateway. | brief |

Table 64: show unified-edge ggsn-pgw subscribers Output Fields (*continued*)

| Field Name | Field Description | Level of Output |
|--------------------------------|---|-----------------|
| APN | Access point name (APN), on the broadband gateway, to which the subscriber is attached. | brief |
| Subscriber Information: | | |
| 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 |
| Time Zone | Time zone to which the subscriber belongs. | extensive |
| (DST) | Daylight savings time applicable within the time zone. | extensive |
| Status | Status of the subscriber; that is, whether the subscriber is a visitor, home subscriber, or a roamer. | 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 |
| 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 |
| PDN Session: | | |
| APN name | Access point name for the Packet Data Network (PDN) session. | extensive |
| IPv4 Address | IPv4 address of the subscriber. | extensive |
| IPv6 Address | IPv6 address of the subscriber. | extensive |
| Direct Tunnel | Status of the GTPv1 direct tunnel: enabled or disabled. | extensive |

Table 64: show unified-edge ggsn-pgw subscribers Output Fields (*continued*)

| Field Name | Field Description | Level of Output |
|-------------------------------|---|------------------|
| Session Duration | Duration of the packet data protocol (PDP) session. | 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. | 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. | 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. | 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. | 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. | extensive |
| Anchor PFE | FPC and PIC slots for the anchor Packet Forwarding Engine for the PDP session. | extensive |
| Session State | State of the subscriber session on the signaling plane. | extensive |
| GTP Version | GTP version used for the control plane. | 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. | 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 |

Table 64: show unified-edge ggsn-pgw subscribers Output Fields (*continued*)

| Field Name | Field Description | Level of Output |
|-----------------------------|---|------------------|
| Bearer: | | |
| NSAPI/EBI | Network Service Access Point Identifier (NSAPI) or the Evolved Packed System Bearer ID (EBI) for the session. | 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 |
| Local Data address | IP address of broadband gateway to which the peer sends the data packets for the PDP context or bearer. | extensive |
| Remote Data address | IP address of the peer to which the broadband gateway sends the data packets for the PDP context or bearer. | 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). | 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. | extensive |
| Bearer State | Represents the state of the subscriber in the forwarding or data plane. This parameter is used internally by the broadband gateway. | extensive |
| Substate | Represents the substate of the subscriber in the forwarding or data plane. This parameter is used internally by the broadband gateway. | 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 |
| 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. | extensive |

Table 64: show unified-edge ggsn-pgw subscribers Output Fields (*continued*)

| Field Name | Field Description | Level of Output |
|-------------------------------------|---|------------------|
| 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—The packet loss priority. | 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). | extensive |
| 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. | extensive |

Table 64: show unified-edge ggsn-pgw subscribers Output Fields (*continued*)

| Field Name | Field Description | Level of Output |
|--------------------------|---|-----------------|
| 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. • 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. • Last statistics 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 ggsn-pgw subscribers | user@host> show unified-edge ggsn-pgw subscribers | IMSI | MSISDN | Subscriber Address | Peer Address | APN |
|--|---|-----------------|------------|--------------------|--------------|------------------|
| | | 605024101215075 | 1896248015 | 31.31.28.5 | 203.1.1.2 | apnv4-gp-dvrf-02 |
| | | 605024101215093 | 1896248033 | 31.31.28.6 | 203.1.1.2 | apnv4-gp-dvrf-02 |
| | | 605024101215074 | 1896248014 | 31.31.56.3 | 203.1.1.2 | apnv4-gp-dvrf-01 |
| | | 605024101215092 | 1896248032 | 31.31.56.4 | 203.1.1.2 | apnv4-gp-dvrf-01 |
| | | 605024101215083 | 1896248023 | 31.31.52.6 | 203.1.1.2 | apnv4-gp-dvrf-02 |
| | | 605024101215089 | 1896248029 | 31.31.92.4 | 203.1.1.2 | apnv4-gp-dvrf-02 |
| | | 605024101215080 | 1896248020 | 31.31.96.2 | 203.1.1.2 | apnv4-gp-dvrf-01 |
| | | 605024101215090 | 1896248030 | 31.31.68.4 | 203.1.1.2 | apnv4-gp-dvrf-01 |
| | | 605024101215088 | 1896248028 | 31.31.68.3 | 203.1.1.2 | apnv4-gp-dvrf-01 |
| | | 605024101215087 | 1896248027 | 31.31.88.8 | 203.1.1.2 | apnv4-gp-dvrf-02 |
| | | 605024101215079 | 1896248019 | 31.31.88.6 | 203.1.1.2 | apnv4-gp-dvrf-02 |
| | | 605024101215085 | 1896248025 | 31.31.88.7 | 203.1.1.2 | apnv4-gp-dvrf-02 |
| | | 605024101215091 | 1896248031 | 31.31.116.8 | 203.1.1.2 | apnv4-gp-dvrf-02 |
| | | 605024101215078 | 1896248018 | 31.31.120.2 | 203.1.1.2 | apnv4-gp-dvrf-01 |

```

605024101215081    1896248021  31.31.116.7    203.1.1.2    apnv4-gp-dvrf-02
605024101215082    1896248022  31.31.45.6     203.1.1.2    apnv4-gp-dvrf-01
605024101215076    1896248016  31.31.45.5     203.1.1.2    apnv4-gp-dvrf-01
605024101215077    1896248017  31.31.134.8    203.1.1.2    apnv4-gp-dvrf-02
605024101215086    1896248026  31.31.45.8     203.1.1.2    apnv4-gp-dvrf-01
605024101215084    1896248024  31.31.45.7     203.1.1.2    apnv4-gp-dvrf-01
[...output truncated...]

```

**show unified-edge
ggsn-pgw subscribers
extensive**

```

user@host> show unified-edge ggsn-pgw subscribers extensive
Subscriber Information:
  IMSI: 605024101215082    IMEI: None
  MSISDN: 1896248022      Time Zone: None    (DST): None
  Status: Visitor
User Location Info:
  MCC: 091    MNC: 050
  LAC: 0x0    CI: 0x0    SAC: 0x0    RAC: 0x0    TAC: 0x0    ECI: 0x0
  RAT Type: E-UTRAN
PDN Session:
  APN name: apnv4-gp-dvrf-01
  IPv4 Address: 31.31.8.18    IPv6 Address: None
  Direct Tunnel: Disabled    Session Duration: 10
  Local Control address: 123.1.1.1 Remote Control address: 11.11.11.2
  TEID Control Local: 0x8001403 TEID Control Remote: 0xf4247
  Peer CSID: 0    Remote CSID: 0
  Addressing scheme: Local    Selection mode: from-ms
  Session PIC: 7 /0 (FPC/PIC) Anchor PFE: 3 /0 (FPC/PIC)
  Session State: Established    GTP Version: 2
  Serving network: MCC: 091 MNC :050
  Negotiated APN AMBR: Downlink: 2000 kbps    Uplink: 2000 kbps
  Requested APN AMBR: Downlink: 2500 kbps    Uplink: 2500 kbps
Bearer:
  NSAPI/EBI: 5    Charging ID: 0x8001403
  Local Data address: 125.1.1.1 Remote Data address: 11.11.11.3
  Local TEID: 0x100803    Remote TEID: 0x1e8487
  Bearer State: Established    Substate: -
  Idle Timeout: 0 min(0 -0,0) AAA Interim Interval: 0 min(0 -0,0)
Negotiated QoS Parameters:
  QCI: 7    ARP: 6 /0 /0 (PL/PVI/PCI)
  Forwarding Class: af2    Loss Priority: high
Requested QoS Parameters:
  QCI :5    ARP : 1 /0 /0 (PL/PVI/PCI)
Charging information:
  Profile ID: 2 Profile name: r8
  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
Rating group information:
  Rating group: 0 Service id: 0
  Action ID: 0x1001403    Trigger profile: 1
  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

Subscriber Information:
  IMSI: 605024101215076      IMEI: None
  MSISDN: 1896248016         Time Zone: None   (DST): None
  Status: Visitor
User Location Info:
  MCC: 091   MNC: 050
  LAC: 0x0   CI: 0x0   SAC: 0x0   RAC: 0x0   TAC: 0x0   ECI: 0x0
  RAT Type: E-UTRAN
PDN Session:
  APN name: apnv4-gp-dvrf-01
  IPv4 Address: 31.31.8.12      IPv6 Address: None
  Direct Tunnel: Disabled      Session Duration: 10
  Local Control address: 123.1.1.1 Remote Control address: 11.11.11.2
  TEID Control Local: 0x8001002 TEID Control Remote: 0xf4241
  Peer CSID: 0                 Remote CSID: 0
  Addressing scheme: Local      Selection mode: from-ms
  Session PIC: 7 /0 (FPC/PIC)   Anchor PFE: 3 /0 (FPC/PIC)
  Session State: Established    GTP Version: 2
  Serving network: MCC: 091   MNC :050
  Negotiated APN AMBR: Downlink: 2000 kbps   Uplink: 2000 kbps
  Requested APN AMBR: Downlink: 2500 kbps   Uplink: 2500 kbps
Bearer:
  NSAPI/EBI: 5                 Charging ID: 0x8001002
  Local Data address: 125.1.1.1 Remote Data address: 11.11.11.3
  Local TEID: 0x101001         Remote TEID: 0x1e8481
  Bearer State: Established     Substate: -
  Idle Timeout: 0 min(0 -0,0)   AAA Interim Interval: 0 min(0 -0,0)
Negotiated QoS Parameters:
  QCI: 7   ARP: 6 /0 /0 (PL/PVI/PCI)
  Forwarding Class: af2         Loss Priority: high
Requested QoS Parameters:
  QCI :5   ARP : 1 /0 /0 (PL/PVI/PCI)
Charging information:
  Profile ID: 2 Profile name: r8
  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
Rating group information:
  Rating group: 0 Service id: 0
  Action ID: 0x1001002      Trigger profile: 1
  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

```

[...output truncated...]

```

show unified-edge ggsn-pgw subscribers fpc-slot 7 pic-slot 0
user@host> show unified-edge ggsn-pgw subscribers fpc-slot 7 pic-slot 0
      IMSI          MSISDN      Subscriber      Peer      APN
      Address      Address
fpc-slot 7 pic-slot 0 605024101215082  1896248022  31.31.8.18    11.11.11.2  apnv4-gp-dvrf-01

```

| | | | | |
|-----------------|------------|------------|------------|------------------|
| 605024101215076 | 1896248016 | 31.31.8.12 | 11.11.11.2 | apnv4-gp-dvrf-01 |
| 605024101215075 | 1896248015 | 31.31.8.11 | 11.11.11.2 | apnv4-gp-dvrf-01 |
| 605024101215077 | 1896248017 | 31.31.8.13 | 11.11.11.2 | apnv4-gp-dvrf-01 |
| 605024101215079 | 1896248019 | 31.31.8.15 | 11.11.11.2 | apnv4-gp-dvrf-01 |
| 605024101215080 | 1896248020 | 31.31.8.16 | 11.11.11.2 | apnv4-gp-dvrf-01 |
| 605024101215083 | 1896248023 | 31.31.8.19 | 11.11.11.2 | apnv4-gp-dvrf-01 |
| 605024101215078 | 1896248018 | 31.31.8.14 | 11.11.11.2 | apnv4-gp-dvrf-01 |
| 605024101215081 | 1896248021 | 31.31.8.17 | 11.11.11.2 | apnv4-gp-dvrf-01 |
| 605024101215084 | 1896248024 | 31.31.8.20 | 11.11.11.2 | apnv4-gp-dvrf-01 |

CHAPTER 32

Charging Operational Commands

clear unified-edge ggsn-pgw charging cdr

| | |
|---------------------------------|--|
| Syntax | <code>clear unified-edge ggsn-pgw charging cdr 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 | Flush out the CDRs from the Service PICs for the configured transport profiles. You can flush out the CDRs for a specific transport-profile only, if needed. However, if you do not specify any transport-profile, then all the CDRs are flushed out for all the transport-profiles. |
| Options | <code>gateway-name <i>name</i></code> —Flush out the CDRs from the Service PICs for the specified gateway. <code>transport-profile-name <i>profile-name</i></code> —Flush out the CDRs from the Service PICS for the specified transport profile only. |
| Required Privilege Level | clear |
| Related Documentation | <ul style="list-style-type: none">• show unified-edge ggsn-pgw charging transfer status on page 946 |
| List of Sample Output | clear unified-edge ggsn-pgw charging cdr gateway-name <i>name</i> on page 876 |
| 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 cdr gateway-name <i>name</i></code> | <code>user@host> clear unified-edge ggsn-pgw charging cdr gateway-name pgw Cleared CDRs</code> |
|--|---|

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 | Flush out those CDRs from the Service PICs that have been sent to CGF or RE, or both, but have not received any acknowledgement from them. You can flush out the CDRs for a specific transport-profile only, if needed. However, if you do not specify any transport-profile, then all the CDRs that are awaiting acknowledgement from CGF or RE are flushed out for all the transport-profiles. |
| Options | <p><code>gateway-name <i>name</i></code>—Flush out the CDRs from the Service PICs that are awaiting acknowledgement from CGF or RE, for the specified gateway.</p> <p><code>transport-profile-name <i>profile-name</i></code>—(Optional) Flush out the CDRs from the Service PICs that are awaiting acknowledgement from CGF or RE, for the specified transport profile only.</p> |
| Required Privilege Level | clear |
| Related Documentation | <ul style="list-style-type: none"> • show unified-edge ggsn-pgw charging transfer status on page 946 |
| List of Sample Output | clear unified-edge ggsn-pgw charging cdr wfa gateway-name <i>name</i> on page 877 |
| 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 cdr wfa gateway-name name</code> | <code>user@host> clear unified-edge ggsn-pgw charging cdr wfa gateway-name pgw Cleared CDRs</code> |
|---|---|

[clear unified-edge ggsn-pgw charging local-persistent-storage statistics](#)

| | |
|---------------------------------|---|
| Syntax | <code>clear unified-edge ggsn-pgw charging local-persistent-storage statistics gateway-name <i>name</i></code> |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Clear the storage statistics of the CDR files on the local RE disk. |
| Options | <code>gateway-name <i>name</i></code> —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 885 |
| List of Sample Output | clear unified-edge ggsn-pgw charging local-persistent-storage statistics gateway-name <i>name</i> on page 878 |
| 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 local-persistent-storage statistics gateway-name <i>name</i></code> | <pre>user@host> clear unified-edge ggsn-pgw charging local-persistent-storage statistics gateway-name pgw Cleared local persistent storage statistics</pre> |
|--|--|

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> > <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. |
| Description | Clear the path management message statistics (between the CDF and the CGF servers). |
| Options | <p>gateway-name <i>name</i>—Clear the path management message statistics for the specified gateway.</p> <p>fpc-slot <i>slot-number</i> pic-slot <i>slot-number</i>—(Optional) Clear the path management message statistics for the specified FPC slot number and PIC slot number only.</p> <p>gtp-peer-addr <i>ipv4-address</i>—(Optional) Clear the path management message statistics for the specified GTP Prime peer only.</p> <p>gtp-peer-name <i>peer-name</i>—(Optional) Clear the path management message statistics for the specified GTP Prime peer only.</p> |
| Required Privilege Level | clear |
| Related Documentation | <ul style="list-style-type: none"> • show unified-edge ggsn-pgw charging path statistics on page 890 |
| List of Sample Output | clear unified-edge ggsn-pgw charging path statistics gateway-name name on page 879 |
| 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 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 transfer statistics. |
| Options | <p><code>gateway-name <i>name</i></code>—Clear the transfer statistics for the specified gateway.</p> <p><code>fpc-slot <i>slot-number</i> pic-slot <i>slot-number</i></code>—(Optional) Clear the transfer statistics for the configured transport profiles for the specific FPC slot number and PIC slot number only.</p> <p><code>transport-profile-name <i>profile-name</i></code>—(Optional) Clear the transfer statistics for the specified transport profile only.</p> |
| Required Privilege Level | clear |
| Related Documentation | <ul style="list-style-type: none">• show unified-edge ggsn-pgw charging transfer statistics on page 935 |
| List of Sample Output | clear unified-edge ggsn-pgw charging transfer statistics gateway-name <i>name</i> on page 880 |
| 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 <i>name</i></code> | <code>user@host> clear unified-edge ggsn-pgw charging transfer statistics gateway-name pgw</code> Cleared 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 884 • request system storage unified-edge charging media stop on page 882 • show unified-edge ggsn-pgw charging local-persistent-storage statistics on page 885 |
| List of Sample Output | request system storage unified-edge charging media start on page 881 |
| 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 | <code>re0 re1</code> —(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 883• request system storage unified-edge charging media start on page 881 |
| List of Sample Output | request system storage unified-edge charging media stop on page 882 |
| 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 882 |
| List of Sample Output | request system storage unified-edge media eject on page 883 |
| 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 | request system storage unified-edge media prepare <no-format> <re0 re1> |
| 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 /opt/mobility. |
| | <div> NOTE: If you do not want to format the existing content on the SSD, you must specify the no-format 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 881• show unified-edge ggsn-pgw charging local-persistent-storage statistics on page 885 |
| List of Sample Output | request system storage unified-edge media prepare on page 884 |
| 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 | user@host> request system storage unified-edge media prepare Creating filesystem Mounting media Media successfully prepared |
|---|--|

show unified-edge ggsn-pgw charging local-persistent-storage statistics

| | |
|---------------------------------|--|
| Syntax | show unified-edge ggsn-pgw charging local-persistent-storage statistics |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Displays the storage statistics of the Charging Data Record (CDR) files on the local Routing Engine disk. |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> clear unified-edge ggsn-pgw charging local-persistent-storage statistics on page 878 |
| List of Sample Output | show unified-edge ggsn-pgw charging local-persistent-storage statistics on page 888 |
| Output Fields | Table 65 on page 885 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 65: show unified-edge ggsn-pgw charging local-persistent-storage statistics Output Fields

| Field Name | Field Description |
|--|---|
| Batch Messages received | The CDRs generated in services PICs are sent to the local Routing Engine disk as batch messages. This counter represents the total number of batch messages sent from services PICs to the Routing Engine disk. |
| Batch Responses sent | The total number of responses sent to the batch messages received. |
| Invalid Messages received | The total number of invalid batch messages sent from services PICs to the Routing Engine disk. |
| Number of temp log files opened | <p>The 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 these can be transferred by 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 separately).</p> |
| Number of journal files opened | Journaling logs the file-write information into the temporary log CDR files. This sanitizes and truncates the temporary log CDR files when the charging daemon comes up after a crash or reboot, in case of inconsistency. For each temporary log CDR file, a separate journal file is opened. This counter indicates the total number of opened journal files. |
| Number of journal files closed | This counter indicates the total number of closed journal files. |

Table 65: show unified-edge ggsn-pgw charging local-persistent-storage statistics Output Fields (continued)

| Field Name | Field Description |
|--|--|
| Number of CDR log files closed | <p>The total number of closed CDR files.</p> <p>Authorized users can use SFTP to transfer these files from the <code>/opt/mobility/charging/ggsn/final_log</code> location.</p> |
| Number of CDR files closed due to file-age | <p>The total number of CDR files closed due to the age of the files reaching the configured limit (or the default limit, when no limit is configured separately).</p> <p>The default value for the file age is 120 minutes.</p> |
| Number of CDR files closed due to file-size | <p>The total number of CDR files closed due to the size of the files reaching the configured limit (or the default limit, when no limit is configured separately).</p> <p>The default file size is 10 MB.</p> |
| Number of CDR files closed due to cdr-count | <p>The total number of CDR files closed due to the maximum number of CDRs added to the files reaching the configured limit.</p> <p>There is no default limit.</p> |
| Abnormal file closures | <p>This counter is incremented when the temporary log CDR file closures are triggered as the charging daemon comes up after a system reboot or crash.</p> |
| Normal file closures | <p>This counter is incremented when the temporary log CDR file closures are triggered due to changes in the configuration, such as a file format change.</p> |
| Number of CDR log files closed in TS_32_297 format | <p>The total number of closed CDR files that are compliant with the format specified in the 32297 technical specification release.</p> |
| Number of CDR log files closed in raw asn1 format | <p>The total number of closed CDR files that are in the raw ASN1 format.</p> |
| Total number of CDRs backed up | <p>The total number of CDRs that have been backed up to the standby Routing Engine.</p> |
| Disk Full messages sent | <p>The total number of messages sent by the Routing Engine to the services PICs to indicate that its disk is full and is unable to accept any more charging data.</p> <p>You may want to use SFTP to transfer the files from the <code>/opt/mobility/charging/ggsn/final_log</code> location to free the 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"> • <code>request system storage unified-edge charging media stop</code> • <code>request system storage unified-edge media eject</code> |
| Disk Full resolve messages sent | <p>When the disk space is freed, the Routing Engine sends messages to the services PICs indicating that it can now receive charging data. This counter indicates the total number of these messages sent.</p> |

Table 65: show unified-edge ggsn-pgw charging local-persistent-storage statistics Output Fields (*continued*)

| Field Name | Field Description |
|--------------------------------------|---|
| Disk Offline messages sent | <p>The 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 is unable to accept any more charging data.</p> <p>You may want to 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 counter indicates the total number of these messages sent. |
| Number of async IO reqs written | This counter is incremented once for every write operation into the temporary log CDR file. |
| Number of CDR storage files on disk | The total number of CDR files stored on the local Routing Engine disk. |
| 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 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 displays after the request system storage unified-edge charging media stop command has been issued but before the disk goes offline. |
| Current storage space in use (MB) | The storage space, in MB, that is currently being used. |
| Available storage space on disk (MB) | The total free space available for storage on the disk, in MB. |
| Total storage space on disk (MB) | The total storage space on the disk, in MB. |
| 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 issued 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 issued and you can take corrective measures to free the disk space.</p> |

Table 65: show unified-edge ggsn-pgw charging local-persistent-storage statistics Output Fields (continued)

| Field Name | Field Description |
|---------------------------------|--|
| Watermark level3 at (MB) | 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. When this limit is reached, an alert (if configured) is issued 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 use SFTP to transfer the files 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. |

The output contains the following information for the temporary CDR files on the router.

| | |
|---------------------------------|--|
| File Name | Name of the temporary CDR file. |
| Journal file name | Name of the journal file associated with the temporary CDR file. |
| Current number of CDRs | The total number of CDRs that have been currently added to the temporary CDR file. |
| Current file size(bytes) | The current size of the temporary CDR file, in bytes. |
| File age trigger(mins) | The duration after which the temporary CDR file is closed, in minutes. The output shows the configured value or the default value, if none is configured. |
| File size trigger(bytes) | The size the temporary CDR file can reach, in bytes, after which it is closed. The output shows the configured value or the default value, if none is configured. |
| CDR count trigger | The maximum number of CDRs that can be added to the temporary CDR file, after which it is closed. The output shows the configured value or the default value, if none is configured. |

Sample Output

```

show unified-edge user@host> show unified-edge ggsn-pgw charging local-persistent-storage statistics
ggsn-pgw charging Charging local-persistent-storage Statistics
local-persistent-storage Batch Messages received : 2
statistics Batch Responses sent : 2
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 : 2

```



```
Disk Full messages sent           : 0
Disk Full resolve messages sent   : 0
Disk Offline messages sent        : 0
Disk Available messages sent      : 1
Number of async IO reqs written   : 2
Number of CDR storage files on disk : 539
Disk space status                  : DISK_AVAILABLE
Current storage space in use(MB)   : 11557
Available storage space on disk(MB) : 22990
Total storage space on disk(MB)    : 34547
Watermark level1 at(MB)           : 13818(40%)
Watermark level2 at(MB)           : 27637(80%)
Watermark level3 at(MB)           : 31092(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 : 2
Current file size(bytes) : 652
File age trigger(mins)  : 120
File size trigger(bytes) : 1048576
CDR count trigger       : 5000
```

show unified-edge ggsn-pgw charging path statistics

| | |
|---------------------------------|--|
| Syntax | <pre>show unified-edge ggsn-pgw charging path statistics <brief detail> <fpc-slot slot-number pic-slot slot-number> <gtp-peer-addr ipv4-address> <gtp-peer-name peer-name></pre> |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Display the path management message statistics (between the Charging Data Function (CDF) and the Charging Gateway Function (CGF) servers). |
| Options | <p>none—(Same as brief) Display the path management message statistics.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>fpc-slot <i>slot-number</i> pic-slot <i>slot-number</i>—(Optional) Display the path management message statistics for the specified Flexible PIC Concentrator (FPC) slot number and PIC slot number only.</p> <p>gtp-peer-addr <i>ipv4-address</i>—(Optional) Display the path management message statistics for the specified general packet radio service (GPRS) tunneling protocol Prime (GTP Prime) peer only.</p> <p>gtp-peer-name <i>peer-name</i>—(Optional) Display the path management message statistics for the specified GTP Prime peer only.</p> |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> clear unified-edge ggsn-pgw charging path statistics on page 879 |
| List of Sample Output | show unified-edge ggsn-pgw charging path statistics on page 893 show unified-edge ggsn-pgw charging path statistics detail on page 897 |
| Output Fields | Table 66 on page 890 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 66: show unified-edge ggsn-pgw charging path statistics Output Fields

| Field Name | Field Description | Level of Output |
|-----------------|---|--------------------|
| 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 |

Table 66: show unified-edge ggsn-pgw charging path statistics Output Fields (*continued*)

| Field Name | Field Description | Level of Output |
|---------------------------------|---|--------------------|
| Echo Requests Rx | Total number of echo requests received by the CDF from a specific 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 it supports. | 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 it supports. | 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 |
| Echo Interval | The configured echo interval in seconds. If no value is configured, then the default value is shown in the output. | All levels none |
| Down Detection Interval | The configured down detect time in seconds. If no value is configured, then the default value is shown in the output. | All levels none |
| Reconnect Time Interval | The configured re-connect time in seconds. If no value is configured, then the default value is shown in the output. | All levels none |
| Destination Port | The configured destination port. If no value is configured, then the default port (3386) is shown in the output. | All levels none |

Table 66: show unified-edge ggsn-pgw charging path statistics Output Fields (*continued*)

| Field Name | Field Description | Level of Output |
|----------------------------------|--|--------------------|
| Pending Queue Size | The configured pending queue size. If no value is configured, then the default value (1024) is shown in the output. | All levels none |
| Path Manager FPC Slot | The FPC slot that manages the path management messages. | All levels none |
| Path Manager PIC Slot | The PIC slot that manages the path management messages. | All levels none |
| Path Manager Port | The port used for path management messages. | All levels none |
| T3 Response Time Interval | The configured T3 response time interval in seconds. If no value is configured, then the default value (5 seconds) is shown in the output. | All levels none |
| Source Interface Valid | Whether the source interface is valid or not. | All levels none |
| GTPP Header Type | The configured header type for the GTP Prime messages. | All levels none |
| N3 Requests | The configured value for N3 requests . If no value is configured, then the default value (3) is shown in the output. | All levels none |
| Local Address | The address of the local loopback source interface from which the GTP Prime packets are sent to the CGF server. | All levels none |
| GTPP Version | The 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 | The configured transport protocol for sending the GTP Prime packets from CDF to the CGF server. | All levels none |
| TCP Port Range Start | The mobile broadband gateway assigns a range of source ports, internally, from which the TCP connection to the CGF server can originate. This number represents the start of this range. | All levels none |
| TCP Port Range End | The mobile broadband gateway assigns a range of source ports, internally, from which the TCP connection to the CGF server can originate. This number represents the end of this range. | All levels none |

Table 66: show unified-edge ggsn-pgw charging path statistics Output Fields (*continued*)

| Field Name | Field Description | Level of Output |
|----------------------|---|-----------------|
| TCP Connection State | Shows the TCP connection state (whether it is established or not) on the Service PIC. | detail |
| FPC/PIC | FPC slot number/PIC slot number. | detail |

Sample Output

```

show unified-edge ggsn-pgw charging path statistics
user@host> show unified-edge ggsn-pgw charging path statistics
Charging Path Statistics

CGF Address           : 13.13.1.1      CGF Server Name       : r7-b1-udp

Echo Requests         Rx: 0          Echo Responses        Tx: 0
Echo Responses        Rx: 0          Echo Requests         Tx: 17
Node-Alive Requests   Rx: 0          Node-Alive Responses   Tx: 0
Version Not Supported Rx: 0          Version Not Supported   Tx: 0
Echo Requests timed out : 16        Echo Interval         : 60
Down Detection Interval : 60        Reconnect Time Interval : 60

Destination Port      : 3386          Pending Queue Size     : 0
Path Manager FPC Slot : 9            Path Manager PIC Slot   : 1
T3 Response Time Interval : 3        Path Manager Port       : 30309

Source Interface Valid : Yes          GTPP Header Type       : short

N3 Requests           : 3            Local Address           : 123.1.1.1

GTPP Version          : V2            Transport Protocol      : UDP

CGF Address           : 14.14.1.1      CGF Server Name       : r7-b2-udp

Echo Requests         Rx: 0          Echo Responses        Tx: 0
Echo Responses        Rx: 9          Echo Requests         Tx: 9
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         : 60
Down Detection Interval : 60        Reconnect Time Interval : 60

Destination Port      : 3386          Pending Queue Size     : 0
Path Manager FPC Slot : 9            Path Manager PIC Slot   : 1
T3 Response Time Interval : 3        Path Manager Port       : 30309

Source Interface Valid : Yes          GTPP Header Type       : short

N3 Requests           : 3            Local Address           : 123.1.1.1

GTPP Version          : V2            Transport Protocol      : UDP

CGF Address           : 15.15.1.1      CGF Server Name       : r7-b3-tcp

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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 0 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30309 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30311 | TCP Port Range End | : 30342 |
| CGF Address | : 16.16.1.1 | CGF Server Name | : r7-b4-tcp |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 0 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30309 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30311 | TCP Port Range End | : 30342 |
| CGF Address | : 13.13.2.2 | CGF Server Name | : r8-b1-udp |
| Echo Requests | Rx: 0 | Echo Responses | Tx: 0 |
| Echo Responses | Rx: 0 | Echo Requests | Tx: 17 |
| Node-Alive Requests | Rx: 0 | Node-Alive Responses | Tx: 0 |
| Version Not Supported | Rx: 0 | Version Not Supported | Tx: 0 |
| Echo Requests timed out | : 16 | Echo Interval | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 0 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30309 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 14.14.2.2 | CGF Server Name | : r8-b2-udp |
| Echo Requests | Rx: 0 | Echo Responses | Tx: 0 |
| Echo Responses | Rx: 9 | Echo Requests | Tx: 9 |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |

| | | | |
|---------------------------|-------------|-------------------------|-------------|
| Destination Port | : 3386 | Pending Queue Size | : 0 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30309 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 15.15.2.2 | CGF Server Name | : r8-b3-tcp |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 0 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30309 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30311 | TCP Port Range End | : 30342 |
| CGF Address | : 16.16.2.2 | CGF Server Name | : r8-b4-tcp |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 0 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30309 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30311 | TCP Port Range End | : 30342 |
| CGF Address | : 13.13.3.3 | CGF Server Name | : |
| r99-b1-udp | | | |
| Echo Requests | Rx: 0 | Echo Responses | Tx: 0 |
| Echo Responses | Rx: 0 | Echo Requests | Tx: 17 |
| Node-Alive Requests | Rx: 0 | Node-Alive Responses | Tx: 0 |
| Version Not Supported | Rx: 0 | Version Not Supported | Tx: 0 |
| Echo Requests timed out | : 16 | Echo Interval | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 0 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |

| | | | |
|---------------------------|-------------|-------------------------|-------------|
| T3 Response Time Interval | : 3 | Path Manager Port | : 30309 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 14.14.3.3 | CGF Server Name | : |
| r99-b2-udp | | | |
| Echo Requests | Rx: 0 | Echo Responses | Tx: 0 |
| Echo Responses | Rx: 9 | Echo Requests | Tx: 9 |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 0 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30309 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 15.15.3.3 | CGF Server Name | : |
| r99-b3-tcp | | | |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 0 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30309 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30311 | TCP Port Range End | : 30342 |
| CGF Address | : 16.16.3.3 | CGF Server Name | : |
| r99-b4-tcp | | | |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 0 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30309 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |


```

N3 Requests           : 3           Local Address           : 123.1.1.1

GTPP Version          : V2           Transport Protocol      : TCP
TCP Port Range Start  : 30311        TCP Port Range End      : 30342

show unified-edge     user@host> show unified-edge ggsn-pgw charging path statistics detail
ggsn-pgw charging     FPC/PIC: 10/0
path statistics detail

CGF Address           : 15.15.1.1    CGF Server Name         : r7-b3-tcp

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 : 60          Reconnect Time Interval : 60

Destination Port       : 3386          Pending Queue Size      : 4096
Path Manager FPC Slot  : 9             Path Manager PIC Slot   : 1
T3 Response Time Interval : 3         Path Manager Port       : 30309

Source Interface Valid : Yes           GTPP Header Type       : short

N3 Requests           : 3           Local Address           : 123.1.1.1

GTPP Version          : V2           Transport Protocol      : TCP
TCP Port Range Start  : 30311        TCP Port Range End      : 30342
TCP Connection State   : Not Established

CGF Address           : 16.16.3.3    CGF Server Name         :
r99-b4-tcp
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 : 60          Reconnect Time Interval : 60

Destination Port       : 3386          Pending Queue Size      : 4096
Path Manager FPC Slot  : 9             Path Manager PIC Slot   : 1
T3 Response Time Interval : 3         Path Manager Port       : 30309

Source Interface Valid : Yes           GTPP Header Type       : short

N3 Requests           : 3           Local Address           : 123.1.1.1

GTPP Version          : V2           Transport Protocol      : TCP
TCP Port Range Start  : 30311        TCP Port Range End      : 30342
TCP Connection State   : Not Established

CGF Address           : 14.14.2.2    CGF Server Name         : r8-b2-udp

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           : 60
Down Detection Interval : 60          Reconnect Time Interval : 60

Destination Port       : 3386          Pending Queue Size      : 4096

```

| | | | |
|---------------------------|-------------|-------------------------|-------------|
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30309 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 14.14.3.3 | CGF Server Name | : |
| r99-b2-udp | | | |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30309 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 13.13.3.3 | CGF Server Name | : |
| r99-b1-udp | | | |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30309 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 16.16.2.2 | CGF Server Name | : r8-b4-tcp |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30309 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |

```

N3 Requests           : 3           Local Address           : 123.1.1.1

GTPP Version          : V2           Transport Protocol    : TCP
TCP Port Range Start  : 30311        TCP Port Range End    : 30342
TCP Connection State   : Not Established

CGF Address           : 15.15.3.3    CGF Server Name       :
r99-b3-tcp
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 : 60          Reconnect Time Interval : 60

Destination Port      : 3386          Pending Queue Size     : 4096
Path Manager FPC Slot : 9             Path Manager PIC Slot  : 1
T3 Response Time Interval : 3         Path Manager Port      : 30309

Source Interface Valid : Yes          GTPP Header Type      : short

N3 Requests           : 3           Local Address           : 123.1.1.1

GTPP Version          : V2           Transport Protocol    : TCP
TCP Port Range Start  : 30311        TCP Port Range End    : 30342
TCP Connection State   : Not Established

CGF Address           : 14.14.1.1    CGF Server Name       : r7-b2-udp

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         : 60
Down Detection Interval : 60          Reconnect Time Interval : 60

Destination Port      : 3386          Pending Queue Size     : 4096
Path Manager FPC Slot : 9             Path Manager PIC Slot  : 1
T3 Response Time Interval : 3         Path Manager Port      : 30309

Source Interface Valid : Yes          GTPP Header Type      : short

N3 Requests           : 3           Local Address           : 123.1.1.1

GTPP Version          : V2           Transport Protocol    : UDP

CGF Address           : 16.16.1.1    CGF Server Name       : r7-b4-tcp

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 : 60          Reconnect Time Interval : 60

Destination Port      : 3386          Pending Queue Size     : 4096
Path Manager FPC Slot : 9             Path Manager PIC Slot  : 1
T3 Response Time Interval : 3         Path Manager Port      : 30309

Source Interface Valid : Yes          GTPP Header Type      : short

```

| | | | |
|---------------------------|-------------------|-------------------------|-------------|
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30311 | TCP Port Range End | : 30342 |
| TCP Connection State | : Not Established | | |
| CGF Address | : 13.13.1.1 | CGF Server Name | : r7-b1-udp |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30309 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 15.15.2.2 | CGF Server Name | : r8-b3-tcp |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30309 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30311 | TCP Port Range End | : 30342 |
| TCP Connection State | : Not Established | | |
| CGF Address | : 13.13.2.2 | CGF Server Name | : r8-b1-udp |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30309 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |

| | | | |
|---------------------------|-------------------|-------------------------|-------------|
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| FPC/PIC: 10/1 | | | |
| CGF Address | : 15.15.1.1 | CGF Server Name | : r7-b3-tcp |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30343 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30345 | TCP Port Range End | : 30376 |
| TCP Connection State | : Not Established | | |
| CGF Address | : 16.16.3.3 | CGF Server Name | : |
| r99-b4-tcp | | | |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30343 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30345 | TCP Port Range End | : 30376 |
| TCP Connection State | : Not Established | | |
| CGF Address | : 14.14.2.2 | CGF Server Name | : r8-b2-udp |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30343 |

| | | | |
|---------------------------|-------------|-------------------------|-------------|
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 14.14.3.3 | CGF Server Name | : |
| r99-b2-udp | | | |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30343 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 13.13.3.3 | CGF Server Name | : |
| r99-b1-udp | | | |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30343 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 16.16.2.2 | CGF Server Name | : r8-b4-tcp |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30343 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |

```

GTPP Version           : V2           Transport Protocol      : TCP
TCP Port Range Start   : 30345        TCP Port Range End       : 30376
TCP Connection State    : Not Established

CGF Address            : 15.15.3.3    CGF Server Name          :
r99-b3-tcp
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 : 60          Reconnect Time Interval  : 60

Destination Port       : 3386          Pending Queue Size       : 4096
Path Manager FPC Slot  : 9             Path Manager PIC Slot    : 1
T3 Response Time Interval : 3          Path Manager Port        : 30343

Source Interface Valid  : Yes           GTPP Header Type        : short

N3 Requests            : 3             Local Address            : 123.1.1.1

GTPP Version           : V2           Transport Protocol      : TCP
TCP Port Range Start   : 30345        TCP Port Range End       : 30376
TCP Connection State    : Not Established

CGF Address            : 14.14.1.1    CGF Server Name          : r7-b2-udp

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            : 60
Down Detection Interval : 60          Reconnect Time Interval  : 60

Destination Port       : 3386          Pending Queue Size       : 4096
Path Manager FPC Slot  : 9             Path Manager PIC Slot    : 1
T3 Response Time Interval : 3          Path Manager Port        : 30343

Source Interface Valid  : Yes           GTPP Header Type        : short

N3 Requests            : 3             Local Address            : 123.1.1.1

GTPP Version           : V2           Transport Protocol      : UDP

CGF Address            : 16.16.1.1    CGF Server Name          : r7-b4-tcp

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 : 60          Reconnect Time Interval  : 60

Destination Port       : 3386          Pending Queue Size       : 4096
Path Manager FPC Slot  : 9             Path Manager PIC Slot    : 1
T3 Response Time Interval : 3          Path Manager Port        : 30343

Source Interface Valid  : Yes           GTPP Header Type        : short

N3 Requests            : 3             Local Address            : 123.1.1.1

```

| | | | |
|---------------------------|-------------------|-------------------------|-------------|
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30345 | TCP Port Range End | : 30376 |
| TCP Connection State | : Not Established | | |
| CGF Address | : 13.13.1.1 | CGF Server Name | : r7-b1-udp |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30343 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 15.15.2.2 | CGF Server Name | : r8-b3-tcp |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30343 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30345 | TCP Port Range End | : 30376 |
| TCP Connection State | : Not Established | | |
| CGF Address | : 13.13.2.2 | CGF Server Name | : r8-b1-udp |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30343 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |


```

      GTPP Version           : V2           Transport Protocol      : UDP
      FPC/PIC: 7/0

      CGF Address            : 15.15.1.1    CGF Server Name           : r7-b3-tcp

      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 : 60          Reconnect Time Interval   : 60

      Destination Port        : 3386         Pending Queue Size        : 4096
      Path Manager FPC Slot   : 9            Path Manager PIC Slot     : 1
      T3 Response Time Interval : 3         Path Manager Port         : 30275

      Source Interface Valid  : Yes          GTPP Header Type         : short

      N3 Requests            : 3            Local Address             : 123.1.1.1

      GTPP Version           : V2           Transport Protocol      : TCP
      TCP Port Range Start    : 30277        TCP Port Range End       : 30308
      TCP Connection State    : Not Established

      CGF Address            : 16.16.3.3    CGF Server Name           :
      r99-b4-tcp
      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 : 60          Reconnect Time Interval   : 60

      Destination Port        : 3386         Pending Queue Size        : 4096
      Path Manager FPC Slot   : 9            Path Manager PIC Slot     : 1
      T3 Response Time Interval : 3         Path Manager Port         : 30275

      Source Interface Valid  : Yes          GTPP Header Type         : short

      N3 Requests            : 3            Local Address             : 123.1.1.1

      GTPP Version           : V2           Transport Protocol      : TCP
      TCP Port Range Start    : 30277        TCP Port Range End       : 30308
      TCP Connection State    : Not Established

      CGF Address            : 14.14.2.2    CGF Server Name           : r8-b2-udp

      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             : 60
      Down Detection Interval : 60          Reconnect Time Interval   : 60

      Destination Port        : 3386         Pending Queue Size        : 4096
      Path Manager FPC Slot   : 9            Path Manager PIC Slot     : 1
      T3 Response Time Interval : 3         Path Manager Port         : 30275

      Source Interface Valid  : Yes          GTPP Header Type         : short

      N3 Requests            : 3            Local Address             : 123.1.1.1

```

| | | | |
|---------------------------|-------------------|-------------------------|-------------|
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 14.14.3.3 | CGF Server Name | : |
| r99-b2-udp | | | |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30275 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 13.13.3.3 | CGF Server Name | : |
| r99-b1-udp | | | |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30275 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 16.16.2.2 | CGF Server Name | : r8-b4-tcp |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30275 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30277 | TCP Port Range End | : 30308 |
| TCP Connection State | : Not Established | | |

```

CGF Address          : 15.15.3.3      CGF Server Name      :
r99-b3-tcp
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 : 60          Reconnect Time Interval : 60

Destination Port      : 3386          Pending Queue Size     : 4096
Path Manager FPC Slot : 9             Path Manager PIC Slot   : 1
T3 Response Time Interval : 3        Path Manager Port       : 30275

Source Interface Valid : Yes          GTPP Header Type       : short

N3 Requests           : 3             Local Address           : 123.1.1.1

GTPP Version          : V2            Transport Protocol      : TCP
TCP Port Range Start   : 30277        TCP Port Range End      : 30308
TCP Connection State    : Not Established

CGF Address          : 14.14.1.1      CGF Server Name      : r7-b2-udp

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
---(backing up)---
Destination Port      : 3386          Pending Queue Size     : 4096
Path Manager FPC Slot : 9             Path Manager PIC Slot   : 1
T3 Response Time Interval : 3        Path Manager Port       : 30275

Source Interface Valid : Yes          GTPP Header Type       : short

N3 Requests           : 3             Local Address           : 123.1.1.1

GTPP Version          : V2            Transport Protocol      : UDP

CGF Address          : 16.16.2.2      CGF Server Name      : r8-b4-tcp

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 : 60          Reconnect Time Interval : 60

Destination Port      : 3386          Pending Queue Size     : 4096
Path Manager FPC Slot : 9             Path Manager PIC Slot   : 1
T3 Response Time Interval : 3        Path Manager Port       : 30275

Source Interface Valid : Yes          GTPP Header Type       : short

N3 Requests           : 3             Local Address           : 123.1.1.1

GTPP Version          : V2            Transport Protocol      : TCP
TCP Port Range Start   : 30277        TCP Port Range End      : 30308
TCP Connection State    : Not Established

CGF Address          : 15.15.3.3      CGF Server Name      :

```

```

r99-b3-tcp
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 : 60      Reconnect Time Interval : 60

Destination Port      : 3386      Pending Queue Size : 4096
Path Manager FPC Slot : 9         Path Manager PIC Slot : 1
T3 Response Time Interval : 3     Path Manager Port    : 30275

Source Interface Valid : Yes      GTPP Header Type   : short

N3 Requests          : 3          Local Address       : 123.1.1.1

GTPP Version          : V2         Transport Protocol   : TCP
TCP Port Range Start  : 30277      TCP Port Range End   : 30308
TCP Connection State   : Not Established

CGF Address           : 14.14.1.1   CGF Server Name      : r7-b2-udp

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      : 60
Down Detection Interval : 60      Reconnect Time Interval : 60

Destination Port      : 3386      Pending Queue Size : 4096
Path Manager FPC Slot : 9         Path Manager PIC Slot : 1
T3 Response Time Interval : 3     Path Manager Port    : 30275

Source Interface Valid : Yes      GTPP Header Type   : short

N3 Requests          : 3          Local Address       : 123.1.1.1

GTPP Version          : V2         Transport Protocol   : UDP

CGF Address           : 16.16.1.1   CGF Server Name      : r7-b4-tcp

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 : 60      Reconnect Time Interval : 60

Destination Port      : 3386      Pending Queue Size : 4096
Path Manager FPC Slot : 9         Path Manager PIC Slot : 1
T3 Response Time Interval : 3     Path Manager Port    : 30275

Source Interface Valid : Yes      GTPP Header Type   : short

N3 Requests          : 3          Local Address       : 123.1.1.1

GTPP Version          : V2         Transport Protocol   : TCP
TCP Port Range Start  : 30277      TCP Port Range End   : 30308
TCP Connection State   : Not Established

CGF Address           : 13.13.1.1   CGF Server Name      : r7-b1-udp

```

| | | | |
|---------------------------|-------------------|-------------------------|-------------|
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| | | | |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30275 |
| | | | |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| | | | |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| | | | |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| | | | |
| CGF Address | : 15.15.2.2 | CGF Server Name | : r8-b3-tcp |
| | | | |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| | | | |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30275 |
| | | | |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| | | | |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| | | | |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30277 | TCP Port Range End | : 30308 |
| TCP Connection State | : Not Established | | |
| | | | |
| CGF Address | : 13.13.2.2 | CGF Server Name | : r8-b1-udp |
| | | | |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| | | | |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30275 |
| | | | |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| | | | |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| | | | |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| FPC/PIC: 7/1 | | | |
| | | | |
| CGF Address | : 15.15.1.1 | CGF Server Name | : r7-b3-tcp |

| | | | |
|---------------------------|-------------------|-------------------------|-------------|
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30241 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30243 | TCP Port Range End | : 30274 |
| TCP Connection State | : Not Established | | |
| CGF Address | : 16.16.3.3 | CGF Server Name | : |
| r99-b4-tcp | | | |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30241 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30243 | TCP Port Range End | : 30274 |
| TCP Connection State | : Not Established | | |
| CGF Address | : 14.14.2.2 | CGF Server Name | : r8-b2-udp |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30241 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 14.14.3.3 | CGF Server Name | : |
| r99-b2-udp | | | |

| | | | |
|---------------------------|-------------------|-------------------------|-------------|
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| | | | |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30241 |
| | | | |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| | | | |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| | | | |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| | | | |
| CGF Address | : 13.13.3.3 | CGF Server Name | : |
| r99-b1-udp | | | |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| | | | |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30241 |
| | | | |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| | | | |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| | | | |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| | | | |
| CGF Address | : 16.16.2.2 | CGF Server Name | : r8-b4-tcp |
| | | | |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| | | | |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30241 |
| | | | |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| | | | |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| | | | |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30243 | TCP Port Range End | : 30274 |
| TCP Connection State | : Not Established | | |
| | | | |
| CGF Address | : 15.15.3.3 | CGF Server Name | : |
| r99-b3-tcp | | | |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30241 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30243 | TCP Port Range End | : 30274 |
| TCP Connection State | : Not Established | | |
| CGF Address | : 14.14.1.1 | CGF Server Name | : r7-b2-udp |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30241 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 16.16.1.1 | CGF Server Name | : r7-b4-tcp |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30241 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30243 | TCP Port Range End | : 30274 |
| TCP Connection State | : Not Established | | |
| CGF Address | : 13.13.1.1 | CGF Server Name | : r7-b1-udp |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30241 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 15.15.2.2 | CGF Server Name | : r8-b3-tcp |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30241 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30243 | TCP Port Range End | : 30274 |
| TCP Connection State | : Not Established | | |
| CGF Address | : 13.13.2.2 | CGF Server Name | : r8-b1-udp |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30241 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| FPC/PIC: 8/0 | | | |
| CGF Address | : 15.15.1.1 | CGF Server Name | : r7-b3-tcp |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30309 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30311 | TCP Port Range End | : 30342 |
| TCP Connection State | : Not Established | | |
| CGF Address | : 16.16.3.3 | CGF Server Name | : |
| r99-b4-tcp | | | |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30309 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30311 | TCP Port Range End | : 30342 |
| TCP Connection State | : Not Established | | |
| CGF Address | : 14.14.2.2 | CGF Server Name | : r8-b2-udp |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30309 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 14.14.3.3 | CGF Server Name | : |
| r99-b2-udp | | | |
| 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
Echo Requests timed out : 0
Down Detection Interval : 60

Destination Port : 3386
Path Manager FPC Slot : 9
T3 Response Time Interval : 3

Source Interface Valid : Yes

N3 Requests : 3

GTPP Version : V2

CGF Address : 13.13.3.3
r99-b1-udp
Echo Requests Rx: 0
Echo Responses Rx: 0
Node-Alive Requests Rx: 0
Version Not Supported Rx: 0
Echo Requests timed out : 0
Down Detection Interval : 60

Destination Port : 3386
Path Manager FPC Slot : 9
T3 Response Time Interval : 3

Source Interface Valid : Yes

N3 Requests : 3

GTPP Version : V2

CGF Address : 16.16.2.2
Echo Requests Rx: 0
Echo Responses Rx: 0
Node-Alive Requests Rx: 0
Version Not Supported Rx: 0
Echo Requests timed out : 0
Down Detection Interval : 60

Destination Port : 3386
Path Manager FPC Slot : 9
T3 Response Time Interval : 3

Source Interface Valid : Yes

N3 Requests : 3

GTPP Version : V2
TCP Port Range Start : 30311
TCP Connection State : Not Established

CGF Address : 15.15.3.3
r99-b3-tcp
Echo Requests Rx: 0
Echo Responses Rx: 0
Node-Alive Requests Rx: 0
Version Not Supported Rx: 0
Echo Requests timed out : 0

Version Not Supported Tx: 0
Echo Interval : 60
Reconnect Time Interval : 60

Pending Queue Size : 4096
Path Manager PIC Slot : 1
Path Manager Port : 30309

GTPP Header Type : short

Local Address : 123.1.1.1

Transport Protocol : UDP

CGF Server Name :

Echo Responses Tx: 0
Echo Requests Tx: 0
Node-Alive Responses Tx: 0
Version Not Supported Tx: 0
Echo Interval : 60
Reconnect Time Interval : 60

Pending Queue Size : 4096
Path Manager PIC Slot : 1
Path Manager Port : 30309

GTPP Header Type : short

Local Address : 123.1.1.1

Transport Protocol : UDP

CGF Server Name : r8-b4-tcp

Echo Responses Tx: 0
Echo Requests Tx: 0
Node-Alive Responses Tx: 0
Version Not Supported Tx: 0
Echo Interval : 0
Reconnect Time Interval : 60

Pending Queue Size : 4096
Path Manager PIC Slot : 1
Path Manager Port : 30309

GTPP Header Type : short

Local Address : 123.1.1.1

Transport Protocol : TCP
TCP Port Range End : 30342

CGF Server Name :

Echo Responses Tx: 0
Echo Requests Tx: 0
Node-Alive Responses Tx: 0
Version Not Supported Tx: 0
Echo Interval : 0

```

| | | | |
|---------------------------|-------------------|-------------------------|-------------|
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30309 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30311 | TCP Port Range End | : 30342 |
| TCP Connection State | : Not Established | | |
| CGF Address | : 14.14.1.1 | CGF Server Name | : r7-b2-udp |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30309 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 16.16.1.1 | CGF Server Name | : r7-b4-tcp |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30309 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30311 | TCP Port Range End | : 30342 |
| TCP Connection State | : Not Established | | |
| CGF Address | : 13.13.1.1 | CGF Server Name | : r7-b1-udp |
| 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 | : 60 |

```

Down Detection Interval : 60          Reconnect Time Interval : 60

Destination Port        : 3386        Pending Queue Size       : 4096
Path Manager FPC Slot   : 9           Path Manager PIC Slot    : 1
T3 Response Time Interval : 3         Path Manager Port        : 30309

Source Interface Valid  : Yes          GTPP Header Type        : short

N3 Requests            : 3            Local Address            : 123.1.1.1

GTPP Version           : V2           Transport Protocol       : UDP

CGF Address            : 15.15.2.2     CGF Server Name          : r8-b3-tcp

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 : 60          Reconnect Time Interval : 60

Destination Port        : 3386        Pending Queue Size       : 4096
Path Manager FPC Slot   : 9           Path Manager PIC Slot    : 1
T3 Response Time Interval : 3         Path Manager Port        : 30309

Source Interface Valid  : Yes          GTPP Header Type        : short

N3 Requests            : 3            Local Address            : 123.1.1.1

GTPP Version           : V2           Transport Protocol       : TCP
TCP Port Range Start    : 30311       TCP Port Range End      : 30342
TCP Connection State    : Not Established

CGF Address            : 13.13.2.2     CGF Server Name          : r8-b1-udp

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            : 60
Down Detection Interval : 60          Reconnect Time Interval : 60

Destination Port        : 3386        Pending Queue Size       : 4096
Path Manager FPC Slot   : 9           Path Manager PIC Slot    : 1
T3 Response Time Interval : 3         Path Manager Port        : 30309

Source Interface Valid  : Yes          GTPP Header Type        : short

N3 Requests            : 3            Local Address            : 123.1.1.1

GTPP Version           : V2           Transport Protocol       : UDP
FPC/PIC: 8/1

CGF Address            : 15.15.1.1     CGF Server Name          : r7-b3-tcp

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 : 60          Reconnect Time Interval : 60

```

```

Destination Port      : 3386          Pending Queue Size   : 4096
Path Manager FPC Slot : 9             Path Manager PIC Slot : 1
T3 Response Time Interval : 3         Path Manager Port     : 30343

Source Interface Valid : Yes          GTPP Header Type     : short

N3 Requests          : 3             Local Address         : 123.1.1.1

GTPP Version         : V2            Transport Protocol    : TCP
TCP Port Range Start : 30345         TCP Port Range End    : 30376
TCP Connection State  : Not Established

CGF Address          : 16.16.3.3      CGF Server Name       :
r99-b4-tcp
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 : 60         Reconnect Time Interval : 60

Destination Port      : 3386          Pending Queue Size   : 4096
Path Manager FPC Slot : 9             Path Manager PIC Slot : 1
T3 Response Time Interval : 3         Path Manager Port     : 30343

Source Interface Valid : Yes          GTPP Header Type     : short

N3 Requests          : 3             Local Address         : 123.1.1.1

GTPP Version         : V2            Transport Protocol    : TCP
TCP Port Range Start : 30345         TCP Port Range End    : 30376
TCP Connection State  : Not Established

CGF Address          : 14.14.2.2      CGF Server Name       : r8-b2-udp

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         : 60
Down Detection Interval : 60         Reconnect Time Interval : 60

Destination Port      : 3386          Pending Queue Size   : 4096
Path Manager FPC Slot : 9             Path Manager PIC Slot : 1
T3 Response Time Interval : 3         Path Manager Port     : 30343

Source Interface Valid : Yes          GTPP Header Type     : short

N3 Requests          : 3             Local Address         : 123.1.1.1

GTPP Version         : V2            Transport Protocol    : UDP

CGF Address          : 14.14.3.3      CGF Server Name       :
r99-b2-udp
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         : 60
Down Detection Interval : 60         Reconnect Time Interval : 60

```

```

Destination Port      : 3386          Pending Queue Size    : 4096
Path Manager FPC Slot : 9             Path Manager PIC Slot  : 1
T3 Response Time Interval : 3         Path Manager Port      : 30343

Source Interface Valid : Yes          GTPP Header Type      : short

N3 Requests          : 3             Local Address          : 123.1.1.1

GTPP Version          : V2           Transport Protocol     : UDP

CGF Address           : 13.13.3.3     CGF Server Name        :
r99-b1-udp
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          : 60
Down Detection Interval : 60         Reconnect Time Interval : 60

Destination Port      : 3386          Pending Queue Size    : 4096
Path Manager FPC Slot : 9             Path Manager PIC Slot  : 1
T3 Response Time Interval : 3         Path Manager Port      : 30343

Source Interface Valid : Yes          GTPP Header Type      : short

N3 Requests          : 3             Local Address          : 123.1.1.1

GTPP Version          : V2           Transport Protocol     : UDP

CGF Address           : 16.16.2.2     CGF Server Name        : r8-b4-tcp

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 : 60         Reconnect Time Interval : 60

Destination Port      : 3386          Pending Queue Size    : 4096
Path Manager FPC Slot : 9             Path Manager PIC Slot  : 1
T3 Response Time Interval : 3         Path Manager Port      : 30343

Source Interface Valid : Yes          GTPP Header Type      : short

N3 Requests          : 3             Local Address          : 123.1.1.1

GTPP Version          : V2           Transport Protocol     : TCP
TCP Port Range Start  : 30345        TCP Port Range End     : 30376
TCP Connection State   : Not Established

CGF Address           : 15.15.3.3     CGF Server Name        :
r99-b3-tcp
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 : 60         Reconnect Time Interval : 60

Destination Port      : 3386          Pending Queue Size    : 4096

```

| | | | |
|---------------------------|-------------------|-------------------------|-------------|
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30343 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30345 | TCP Port Range End | : 30376 |
| TCP Connection State | : Not Established | | |
| CGF Address | : 14.14.1.1 | CGF Server Name | : r7-b2-udp |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30343 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 16.16.1.1 | CGF Server Name | : r7-b4-tcp |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30343 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30345 | TCP Port Range End | : 30376 |
| TCP Connection State | : Not Established | | |
| CGF Address | : 13.13.1.1 | CGF Server Name | : r7-b1-udp |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |

| | | | |
|---------------------------|-------------------|-------------------------|-------------|
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30343 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 15.15.2.2 | CGF Server Name | : r8-b3-tcp |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30343 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30345 | TCP Port Range End | : 30376 |
| TCP Connection State | : Not Established | | |
| CGF Address | : 13.13.2.2 | CGF Server Name | : r8-b1-udp |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30343 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| FPC/PIC: 9/0 | | | |
| CGF Address | : 15.15.1.1 | CGF Server Name | : r7-b3-tcp |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |

| | | | |
|---------------------------|-------------------|-------------------------|-------------|
| T3 Response Time Interval | : 3 | Path Manager Port | : 30275 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30277 | TCP Port Range End | : 30308 |
| TCP Connection State | : Not Established | | |
| CGF Address | : 16.16.3.3 | CGF Server Name | : |
| r99-b4-tcp | | | |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30275 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30277 | TCP Port Range End | : 30308 |
| TCP Connection State | : Not Established | | |
| CGF Address | : 14.14.2.2 | CGF Server Name | : r8-b2-udp |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30275 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 14.14.3.3 | CGF Server Name | : |
| r99-b2-udp | | | |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |

```

T3 Response Time Interval : 3          Path Manager Port      : 30275

Source Interface Valid    : Yes        GTPP Header Type       : short

N3 Requests               : 3          Local Address          : 123.1.1.1

GTPP Version              : V2         Transport Protocol      : UDP

CGF Address               : 13.13.3.3  CGF Server Name        :
r99-b1-udp
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           : 60
Down Detection Interval   : 60         Reconnect Time Interval : 60

Destination Port          : 3386        Pending Queue Size      : 4096
Path Manager FPC Slot     : 9          Path Manager PIC Slot   : 1
T3 Response Time Interval : 3          Path Manager Port       : 30275

Source Interface Valid    : Yes        GTPP Header Type       : short

N3 Requests               : 3          Local Address          : 123.1.1.1

GTPP Version              : V2         Transport Protocol      : UDP

CGF Address               : 16.16.2.2  CGF Server Name        : r8-b4-tcp

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   : 60         Reconnect Time Interval : 60

Destination Port          : 3386        Pending Queue Size      : 4096
Path Manager FPC Slot     : 9          Path Manager PIC Slot   : 1
T3 Response Time Interval : 3          Path Manager Port       : 30275

Source Interface Valid    : Yes        GTPP Header Type       : short

N3 Requests               : 3          Local Address          : 123.1.1.1

GTPP Version              : V2         Transport Protocol      : TCP
TCP Port Range Start      : 30277      TCP Port Range End      : 30308
TCP Connection State      : Not Established

CGF Address               : 15.15.3.3  CGF Server Name        :
r99-b3-tcp
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   : 60         Reconnect Time Interval : 60

Destination Port          : 3386        Pending Queue Size      : 4096
Path Manager FPC Slot     : 9          Path Manager PIC Slot   : 1
T3 Response Time Interval : 3          Path Manager Port       : 30275

```

| | | | |
|---------------------------|-------------------|-------------------------|-------------|
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30277 | TCP Port Range End | : 30308 |
| TCP Connection State | : Not Established | | |
| CGF Address | : 14.14.1.1 | CGF Server Name | : r7-b2-udp |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30275 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 16.16.1.1 | CGF Server Name | : r7-b4-tcp |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30275 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30277 | TCP Port Range End | : 30308 |
| TCP Connection State | : Not Established | | |
| CGF Address | : 13.13.1.1 | CGF Server Name | : r7-b1-udp |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30275 |

| | | | |
|---------------------------|-------------------|-------------------------|-------------|
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 15.15.2.2 | CGF Server Name | : r8-b3-tcp |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30275 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30277 | TCP Port Range End | : 30308 |
| TCP Connection State | : Not Established | | |
| CGF Address | : 13.13.2.2 | CGF Server Name | : r8-b1-udp |
| 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 | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30275 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |
| FPC/PIC: 9/1 | | | |
| CGF Address | : 15.15.1.1 | CGF Server Name | : r7-b3-tcp |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30241 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |

```

N3 Requests           : 3           Local Address           : 123.1.1.1

GTPP Version          : V2           Transport Protocol      : TCP
TCP Port Range Start  : 30243        TCP Port Range End      : 30274
TCP Connection State   : Not Established

CGF Address           : 16.16.3.3    CGF Server Name         :
r99-b4-tcp
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 : 60         Reconnect Time Interval : 60

Destination Port       : 3386         Pending Queue Size       : 4096
Path Manager FPC Slot  : 9           Path Manager PIC Slot    : 1
T3 Response Time Interval : 3       Path Manager Port        : 30241

Source Interface Valid : Yes         GTPP Header Type        : short

N3 Requests           : 3           Local Address           : 123.1.1.1

GTPP Version          : V2           Transport Protocol      : TCP
TCP Port Range Start  : 30243        TCP Port Range End      : 30274
TCP Connection State   : Not Established

CGF Address           : 14.14.2.2    CGF Server Name         : r8-b2-udp

Echo Requests         Rx: 0           Echo Responses          Tx: 0
Echo Responses        Rx: 14         Echo Requests           Tx: 14
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           : 60
Down Detection Interval : 60         Reconnect Time Interval : 60

Destination Port       : 3386         Pending Queue Size       : 4096
Path Manager FPC Slot  : 9           Path Manager PIC Slot    : 1
T3 Response Time Interval : 3       Path Manager Port        : 30241

Source Interface Valid : Yes         GTPP Header Type        : short

N3 Requests           : 3           Local Address           : 123.1.1.1

GTPP Version          : V2           Transport Protocol      : UDP

CGF Address           : 14.14.3.3    CGF Server Name         :
r99-b2-udp
Echo Requests         Rx: 0           Echo Responses          Tx: 0
Echo Responses        Rx: 14         Echo Requests           Tx: 14
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           : 60
Down Detection Interval : 60         Reconnect Time Interval : 60

Destination Port       : 3386         Pending Queue Size       : 4096
Path Manager FPC Slot  : 9           Path Manager PIC Slot    : 1
T3 Response Time Interval : 3       Path Manager Port        : 30241

Source Interface Valid : Yes         GTPP Header Type        : short

```

```

N3 Requests           : 3           Local Address       : 123.1.1.1

GTPP Version          : V2           Transport Protocol : UDP

CGF Address           : 13.13.3.3    CGF Server Name     :
r99-b1-udp
Echo Requests         Rx: 0           Echo Responses      Tx: 0
Echo Responses        Rx: 0           Echo Requests       Tx: 28
Node-Alive Requests   Rx: 0           Node-Alive Responses Tx: 0
Version Not Supported Rx: 0           Version Not Supported Tx: 0
Echo Requests timed out : 28         Echo Interval       : 60
Down Detection Interval : 60         Reconnect Time Interval : 60

Destination Port      : 3386         Pending Queue Size   : 4096
Path Manager FPC Slot : 9           Path Manager PIC Slot : 1
T3 Response Time Interval : 3       Path Manager Port     : 30241

Source Interface Valid : Yes         GTPP Header Type     : short

N3 Requests           : 3           Local Address       : 123.1.1.1

GTPP Version          : V2           Transport Protocol : UDP

CGF Address           : 16.16.2.2    CGF Server Name     : r8-b4-tcp

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 : 60         Reconnect Time Interval : 60

Destination Port      : 3386         Pending Queue Size   : 4096
Path Manager FPC Slot : 9           Path Manager PIC Slot : 1
T3 Response Time Interval : 3       Path Manager Port     : 30241

Source Interface Valid : Yes         GTPP Header Type     : short

N3 Requests           : 3           Local Address       : 123.1.1.1

GTPP Version          : V2           Transport Protocol : TCP
TCP Port Range Start  : 30243        TCP Port Range End   : 30274
TCP Connection State   : Not Established

CGF Address           : 15.15.3.3    CGF Server Name     :
r99-b3-tcp
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 : 60         Reconnect Time Interval : 60

Destination Port      : 3386         Pending Queue Size   : 4096
Path Manager FPC Slot : 9           Path Manager PIC Slot : 1
T3 Response Time Interval : 3       Path Manager Port     : 30241

Source Interface Valid : Yes         GTPP Header Type     : short

N3 Requests           : 3           Local Address       : 123.1.1.1

```

```

GTPP Version           : V2           Transport Protocol      : TCP
TCP Port Range Start   : 30243        TCP Port Range End       : 30274
TCP Connection State    : Not Established

CGF Address            : 14.14.1.1    CGF Server Name          : r7-b2-udp

Echo Requests          Rx: 0           Echo Responses           Tx: 0
Echo Responses         Rx: 14          Echo Requests            Tx: 14
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            : 60
Down Detection Interval : 60          Reconnect Time Interval  : 60

Destination Port       : 3386          Pending Queue Size       : 4096
Path Manager FPC Slot  : 9             Path Manager PIC Slot    : 1
T3 Response Time Interval : 3         Path Manager Port        : 30241

Source Interface Valid  : Yes          GTPP Header Type        : short

N3 Requests            : 3             Local Address            : 123.1.1.1

GTPP Version           : V2           Transport Protocol      : UDP

CGF Address            : 16.16.1.1    CGF Server Name          : r7-b4-tcp

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 : 60          Reconnect Time Interval  : 60

Destination Port       : 3386          Pending Queue Size       : 4096
Path Manager FPC Slot  : 9             Path Manager PIC Slot    : 1
T3 Response Time Interval : 3         Path Manager Port        : 30241

Source Interface Valid  : Yes          GTPP Header Type        : short

N3 Requests            : 3             Local Address            : 123.1.1.1

GTPP Version           : V2           Transport Protocol      : TCP
TCP Port Range Start   : 30243        TCP Port Range End       : 30274
TCP Connection State    : Not Established

CGF Address            : 13.13.1.1    CGF Server Name          : r7-b1-udp

Echo Requests          Rx: 0           Echo Responses           Tx: 0
Echo Responses         Rx: 0           Echo Requests            Tx: 28
Node-Alive Requests    Rx: 0           Node-Alive Responses     Tx: 0
Version Not Supported  Rx: 0           Version Not Supported    Tx: 0
Echo Requests timed out : 28          Echo Interval            : 60
Down Detection Interval : 60          Reconnect Time Interval  : 60

Destination Port       : 3386          Pending Queue Size       : 4096
Path Manager FPC Slot  : 9             Path Manager PIC Slot    : 1
T3 Response Time Interval : 3         Path Manager Port        : 30241

Source Interface Valid  : Yes          GTPP Header Type        : short

N3 Requests            : 3             Local Address            : 123.1.1.1

```


| | | | |
|---------------------------|-------------------|-------------------------|-------------|
| GTPP Version | : V2 | Transport Protocol | : UDP |
| CGF Address | : 15.15.2.2 | CGF Server Name | : r8-b3-tcp |
| 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 | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30241 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : TCP |
| TCP Port Range Start | : 30243 | TCP Port Range End | : 30274 |
| TCP Connection State | : Not Established | | |
| CGF Address | : 13.13.2.2 | CGF Server Name | : r8-b1-udp |
| Echo Requests | Rx: 0 | Echo Responses | Tx: 0 |
| Echo Responses | Rx: 0 | Echo Requests | Tx: 28 |
| Node-Alive Requests | Rx: 0 | Node-Alive Responses | Tx: 0 |
| Version Not Supported | Rx: 0 | Version Not Supported | Tx: 0 |
| Echo Requests timed out | : 28 | Echo Interval | : 60 |
| Down Detection Interval | : 60 | Reconnect Time Interval | : 60 |
| Destination Port | : 3386 | Pending Queue Size | : 4096 |
| Path Manager FPC Slot | : 9 | Path Manager PIC Slot | : 1 |
| T3 Response Time Interval | : 3 | Path Manager Port | : 30241 |
| Source Interface Valid | : Yes | GTPP Header Type | : short |
| N3 Requests | : 3 | Local Address | : 123.1.1.1 |
| GTPP Version | : V2 | Transport Protocol | : UDP |

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> <gtp-peer-addr ipv4-address> <gtp-peer-name peer-name></pre> |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Display the status of the configured peers: whether they are connected, down, or still in the process of establishing connection and whether the echo messages are enabled or disabled. |
| 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 <i>slot-number</i> pic-slot <i>slot-number</i>—(Optional) Display the status of the configured peers for the specified FPC slot number and PIC slot number only.</p> <p>gtp-peer-addr <i>ipv4-address</i>—(Optional) Display the status of the configured peers for the specified GTP Prime peer only.</p> <p>gtp-peer-name <i>peer-name</i>—(Optional) Display the status of the configured peers for the specified GTP Prime peer only.</p> |
| Required Privilege Level | view |
| List of Sample Output | show unified-edge ggsn-pgw charging path status on page 931 show unified-edge ggsn-pgw charging path status detail on page 931 |
| Output Fields | Table 67 on page 930 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 67: show unified-edge ggsn-pgw charging path status Output Fields

| Field Name | Field Description | Level of Output |
|---------------|---|-----------------|
| Peer-Address | The address of the CGF server (GTP Prime peer). | All levels |
| | | none |
| Peer-Name | The name of the CGF server (GTP Prime peer). | All levels |
| | | none |
| Local-Address | The 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 |

Table 67: show unified-edge ggsn-pgw charging path status Output Fields (*continued*)

| Field Name | Field Description | Level of Output |
|------------|---|-----------------|
| Status | The status of the CGF server. The possible values are: | All levels |
| | <ul style="list-style-type: none"> • Connected • Down • In-Progress | none |
| Echo | Whether echo messages are enabled. The possible values are: | All levels |
| | <ul style="list-style-type: none"> • Enabled or Disabled, for UDP connections • N/A, for TCP connections | none |
| Cause | Probable cause for the current status of the CGF peer. | detail |
| FPC/PIC | FPC slot number/PIC slot number. | detail |

Sample Output

```

show unified-edge user@host> show unified-edge ggsn-pgw charging path status
ggsn-pgw charging
path status      Peer-Addr      Peer-Name      Local-Address   Status          Echo
4.4.4.4         peer3          91.92.1.5      Down            N/A
3.3.3.3         peer2          91.92.1.5      Down            N/A
2.2.2.2         peer1          91.92.1.5      Connected       N/A

```

```

show unified-edge user@host> show unified-edge ggsn-pgw charging path status detail
ggsn-pgw charging
path status detail Charging Path Status

```

```

FPC/PIC 0/0
Peer-Address 4.4.4.4
Peer-Name    peer3
Local-Address 91.92.1.5
Status       Down
Cause        Server Not Responding
Echo         N/A

Peer-Address 3.3.3.3
Peer-Name    peer2
Local-Address 91.92.1.5
Status       Down
Cause        Server Not Responding
Echo         N/A

Peer-Address 2.2.2.2
Peer-Name    peer1
Local-Address 91.92.1.5
Status       Connected
Echo         N/A

```

show unified-edge ggsn-pgw charging service-mode

| | |
|---------------------------------|---|
| Syntax | <pre>show unified-edge ggsn-pgw charging service-mode <brief detail> <charging-profile <i>profile-name</i>> <gateway <i>gateway-name</i>> <transport-profile <i>profile-name</i>></pre> |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Display the mode in which the charging or transport profile is currently operating in. |
| Options | <p>none—(Same as brief) Display the mode in which the profile is currently operating in.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>charging-profile <i>profile-name</i>—Display the mode in which the charging profile is currently operating in.</p> <p>gateway <i>gateway-name</i>—Display the mode in which the charging profile or transport profile is currently operating in for the specified gateway.</p> <p>transport-profile <i>profile-name</i>—Display the mode in which the transport profile is currently operating in.</p> |
| Required Privilege Level | view |
| List of Sample Output | <p>show unified-edge ggsn-pgw charging service-mode gateway <i>gateway-name</i> charging-profile <i>profile-name</i> on page 933</p> <p>show unified-edge ggsn-pgw charging service-mode gateway <i>gateway-name</i> charging-profile <i>profile-name</i> detail on page 933</p> <p>show unified-edge ggsn-pgw charging service-mode gateway <i>gateway-name</i> transport-profile <i>profile-name</i> on page 933</p> <p>show unified-edge ggsn-pgw charging service-mode gateway <i>gateway-name</i> transport-profile <i>profile-name</i> detail on page 934</p> |
| Output Fields | Table 68 on page 932 lists the output fields for the show unified-edge ggsn-pgw charging service-mode gateway <i>gateway-name</i> command. Output fields are listed in the approximate order in which they appear. |

Table 68: show unified-edge ggsn-pgw charging service-mode gateway *gateway-name* Output Fields

| Field Name | Field Description | Level of Output |
|--------------|---------------------|--------------------|
| Profile Name | Name of the profile | All levels none |

Table 68: show unified-edge ggsn-pgw charging service-mode gateway gateway-name Output Fields (*continued*)

| Field Name | Field Description | Level of Output |
|---|--|-------------------------------|
| Service Mode | <p>The mode in which the profile is currently operating in. The possible values are:</p> <ul style="list-style-type: none"> MM Active Phase—In this mode, you can make changes to any of the configuration options within the charging-profiles or transport-profiles hierarchy. MM In/Out Phase—In this mode, you can make changes to any of the configuration options within: <ul style="list-style-type: none"> The charging-profiles hierarchy except for the CDR profile, transport profile, trigger profile, or profile-id configuration. The transport-profiles hierarchy except for the cdr-release configuration. Operational—The system is still under operational mode and not under maintenance mode. You may want to use the following commands to put the charging or transport profile under maintenance mode: 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 | <p>All levels</p> <p>none</p> |
| 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 gateway-name charging-profile profile-name
user@host> show unified-edge ggsn-pgw charging service-mode gateway PGW charging-profile
juniper
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.

Profile Name          Service Mode
juniper               Maintenance - Active Phase

show unified-edge ggsn-pgw charging service-mode gateway gateway-name charging-profile profile-name detail
user@host> show unified-edge ggsn-pgw charging service-mode gateway PGW charging-profile
juniper detail
Service Mode Status
Profile Name       : juniper
Service Mode       : Maintenance - Active Phase

show unified-edge ggsn-pgw charging service-mode gateway gateway-name
user@host> show unified-edge ggsn-pgw charging service-mode gateway PGW transport-profile
trans_p
Maintenance Mode
  MM Active Phase - System is ready to accept configuration changes for all
                    attributes of this object and its sub-hierarchies.

```


show unified-edge ggsn-pgw charging transfer statistics

| | |
|---------------------------------|---|
| Syntax | show unified-edge ggsn-pgw charging transfer statistics <brief detail> <fpc-slot <i>slot-number</i> pic-slot <i>slot-number</i> > <transport-profile-name <i>profile-name</i> > |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Display the transfer statistics for the configured transport profiles. |
| Options | <p>none—(Same as brief) Display the transfer statistics for the configured transport profiles.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>fpc-slot <i>slot-number</i> pic-slot <i>slot-number</i>—(Optional) Display the transfer statistics for the specified FPC slot number and PIC slot number only.</p> <p>transport-profile-name <i>profile-name</i>—(Optional) Display the transfer statistics for the specified transport profile only.</p> |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> • clear unified-edge ggsn-pgw charging transfer statistics on page 880 |
| List of Sample Output | show unified-edge ggsn-pgw charging transfer statistics on page 937 show unified-edge ggsn-pgw charging transfer statistics detail on page 938 |
| Output Fields | Table 69 on page 935 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. |

Table 69: show unified-edge ggsn-pgw charging transfer statistics Output Fields

| Field Name | Field Description | Level of Output |
|--------------------------------|---|--------------------|
| Transport-Profile | Name of the transport profile. | All levels none |
| Redirection Requests Rx | <p>Total number of redirection request messages received by the CDF from the CGF server.</p> <p>The CGF server can send these messages to inform CDF that:</p> <ul style="list-style-type: none"> • It is about to stop service (maybe due to some error condition or for maintenance). • The next node in the chain (such as a billing server) has lost connection to this CGF server. | All levels none |

Table 69: show unified-edge ggsn-pgw charging transfer statistics Output Fields (*continued*)

| Field Name | Field Description | Level of Output |
|------------------------------------|--|------------------------|
| Redirection Responses Tx | Total number of redirection response messages transmitted as responses to the redirection requests received. This message gives an indication whether a redirection request message was successful. | All levels none |
| DRT Responses Rx | Total number of DRT response messages received for the DRT request messages sent. This message gives an indication whether a DRT request message was successful. | All levels none |
| DRT Requests Tx | Total number of DRT request messages transmitted to the CGF server. These messages are used for the transfer of CDRs from the CDF to the CGF server. | All levels none |
| DRT successful Responses Rx | Total number of successful DRT response messages received for the DRT request messages sent. | All levels none |
| DRT Error Responses Rx | Total number of DRT error response messages received for the DRT request messages sent. | All levels none |
| DRT Requests timed out | Total number of DRT requests sent that got timed out before receiving any responses from the CGF server. | All levels none |
| CGF Switch Back Times | Total number of times the CGF servers were switched. It is an indication of how many times the CGF servers were either offline or closed for maintenance. | All levels none |
| Batch Requests Tx | Total number of batch requests transmitted from Service PICs, for a transport profile. | All levels none |
| Batch Response Errors Rx | Total number of error responses sent by RE to the Service PICs for the batch requests messages received. | All levels none |
| Batch CDR's Tx | Total number of CDRs transmitted from Service PICs to RE. | All levels none |
| CDR Count | Total number of CDRs transmitted to the CGF server. | All levels none |
| Total WFA | Total number of request messages awaiting acknowledgements from either RE or the CGF server. | All levels none |
| FPC/PIC | FPC slot number/PIC slot number. | detail |

Sample Output

```

show unified-edge ggsn-pgw charging transfer statistics
user@host> show unified-edge ggsn-pgw charging transfer statistics
Charging Transfer Statistics
Transport-Profile : R7-1
  Redirection Requests      Rx: 0      Redirection Responses      Tx: 0
  DRT Responses            Rx: 15142   DRT Requests                Tx: 43785
  DRT successful Responses Rx: 15142   DRT Error Responses         Rx: 0
  DRT Requests timed out   : 312891   CGF Switch Back Times      : 88
  Batch Requests           Tx: 599     Batch Response Errors       Rx: 0
  Batch CDR's              Tx: 17862   CDR Count                   : 279651
  Total WFA                 : 1

Transport-Profile : R7-2
  Redirection Requests      Rx: 0      Redirection Responses      Tx: 0
  DRT Responses            Rx: 1185   DRT Requests                Tx: 5301
  DRT successful Responses Rx: 1185   DRT Error Responses         Rx: 0
  DRT Requests timed out   : 42069   CGF Switch Back Times      : 203
  Batch Requests           Tx: 115     Batch Response Errors       Rx: 0
  Batch CDR's              Tx: 1244   CDR Count                   : 23745
  Total WFA                 : 1

Transport-Profile : R7-3
  Redirection Requests      Rx: 0      Redirection Responses      Tx: 0
  DRT Responses            Rx: 565     DRT Requests                Tx: 1489
  DRT successful Responses Rx: 565     DRT Error Responses         Rx: 0
  DRT Requests timed out   : 9903     CGF Switch Back Times      : 104
  Batch Requests           Tx: 65       Batch Response Errors       Rx: 0
  Batch CDR's              Tx: 480     CDR Count                   : 6980
  Total WFA                 : 0

Transport-Profile : R8-1
  Redirection Requests      Rx: 0      Redirection Responses      Tx: 0
  DRT Responses            Rx: 28056   DRT Requests                Tx: 45223
  DRT successful Responses Rx: 28056   DRT Error Responses         Rx: 0
  DRT Requests timed out   : 164971   CGF Switch Back Times      : 86
  Batch Requests           Tx: 829     Batch Response Errors       Rx: 0
  Batch CDR's              Tx: 17993   CDR Count                   : 153550
  Total WFA                 : 2

Transport-Profile : R8-2
  Redirection Requests      Rx: 0      Redirection Responses      Tx: 0
  DRT Responses            Rx: 55727   DRT Requests                Tx: 80117
  DRT successful Responses Rx: 55727   DRT Error Responses         Rx: 0
  DRT Requests timed out   : 358052   CGF Switch Back Times      : 41
  Batch Requests           Tx: 1582   Batch Response Errors       Rx: 0
  Batch CDR's              Tx: 38041   CDR Count                   : 278198
  Total WFA                 : 1

Transport-Profile : R8-3
  Redirection Requests      Rx: 0      Redirection Responses      Tx: 0
  DRT Responses            Rx: 581     DRT Requests                Tx: 1462
  DRT successful Responses Rx: 581     DRT Error Responses         Rx: 0
  DRT Requests timed out   : 8314     CGF Switch Back Times      : 62
  Batch Requests           Tx: 123     Batch Response Errors       Rx: 0
  Batch CDR's              Tx: 753     CDR Count                   : 4900
  Total WFA                 : 0

Transport-Profile : R99-1
  Redirection Requests      Rx: 0      Redirection Responses      Tx: 0

```

| | | | |
|--------------------------|-----------|-----------------------|-----------|
| DRT Responses | Rx: 14293 | DRT Requests | Tx: 18100 |
| DRT successful Responses | Rx: 14293 | DRT Error Responses | Rx: 0 |
| DRT Requests timed out | : 32751 | CGF Switch Back Times | : 29 |
| Batch Requests | Tx: 579 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 17594 | CDR Count | : 125217 |
| Total WFA | : 1 | | |

Transport-Profile : R99-2

| | | | |
|--------------------------|-----------|-----------------------|-----------|
| Redirection Requests | Rx: 0 | Redirection Responses | Tx: 0 |
| DRT Responses | Rx: 14736 | DRT Requests | Tx: 28530 |
| DRT successful Responses | Rx: 14736 | DRT Error Responses | Rx: 0 |
| DRT Requests timed out | : 129291 | CGF Switch Back Times | : 112 |
| Batch Requests | Tx: 643 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 18325 | CDR Count | : 159738 |
| Total WFA | : 1 | | |

**show unified-edge
ggsn-pgw charging
transfer statistics
detail**

user@host> show unified-edge ggsn-pgw charging transfer statistics detail

Charging Transfer Statistics

FPC/PIC: 10/0

Transport-profile : R7-3

| | | | |
|--------------------------|-------|-----------------------|-------|
| Redirection Requests | Rx: 0 | 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 | : 29 | CGF Switch Back Times | : 4 |
| Batch Requests | Tx: 0 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 0 | CDR Count | : 10 |
| Total WFA | : 1 | | |

Transport-profile : R99-2

| | | | |
|--------------------------|-------|-----------------------|-------|
| Redirection Requests | Rx: 0 | 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 | : 9 | CGF Switch Back Times | : 3 |
| Batch Requests | Tx: 1 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 7 | CDR Count | : 32 |
| Total WFA | : 0 | | |

Transport-profile : R8-3

| | | | |
|--------------------------|-------|-----------------------|-------|
| 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 | : 1 |
| Batch Requests | Tx: 0 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 0 | CDR Count | : 0 |
| Total WFA | : 0 | | |

Transport-profile : R8-1

| | | | |
|--------------------------|--------|-----------------------|-------|
| 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 | : 1 |
| Batch Requests | Tx: 1 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 21 | CDR Count | : 21 |
| Total WFA | : 1 | | |

Transport-profile : R7-1

| | | | |
|--------------------------|-------|-----------------------|--------|
| Redirection Requests | Rx: 0 | Redirection Responses | Tx: 0 |
| DRT Responses | Rx: 0 | DRT Requests | Tx: 88 |
| DRT successful Responses | Rx: 0 | DRT Error Responses | Rx: 0 |
| DRT Requests timed out | : 456 | CGF Switch Back Times | : 3 |
| Batch Requests | Tx: 1 | Batch Response Errors | Rx: 0 |

| | | | |
|---------------------------|--------|-----------------------|--------|
| Batch CDR's | Tx: 28 | CDR Count | : 556 |
| Total WFA | : 0 | | |
| Transport-profile : R99-1 | | | |
| 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 | : 1 |
| Batch Requests | Tx: 1 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 14 | CDR Count | : 14 |
| Total WFA | : 1 | | |
| Transport-profile : R7-2 | | | |
| Redirection Requests | Rx: 0 | Redirection Responses | Tx: 0 |
| DRT Responses | Rx: 0 | DRT Requests | Tx: 98 |
| DRT successful Responses | Rx: 0 | DRT Error Responses | Rx: 0 |
| DRT Requests timed out | : 834 | CGF Switch Back Times | : 6 |
| Batch Requests | Tx: 1 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 21 | CDR Count | : 511 |
| Total WFA | : 25 | | |
| Transport-profile : R8-2 | | | |
| 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 | : 1 |
| Batch Requests | Tx: 1 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 7 | CDR Count | : 7 |
| Total WFA | : 1 | | |
| FPC/PIC: 10/1 | | | |
| Transport-profile : R7-3 | | | |
| Redirection Requests | Rx: 0 | Redirection Responses | Tx: 0 |
| DRT Responses | Rx: 0 | DRT Requests | Tx: 1 |
| DRT successful Responses | Rx: 0 | DRT Error Responses | Rx: 0 |
| DRT Requests timed out | : 9 | CGF Switch Back Times | : 2 |
| Batch Requests | Tx: 1 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 7 | CDR Count | : 12 |
| Total WFA | : 1 | | |
| Transport-profile : R99-2 | | | |
| Redirection Requests | Rx: 0 | Redirection Responses | Tx: 0 |
| DRT Responses | Rx: 0 | DRT Requests | Tx: 1 |
| DRT successful Responses | Rx: 0 | DRT Error Responses | Rx: 0 |
| DRT Requests timed out | : 2 | CGF Switch Back Times | : 3 |
| Batch Requests | Tx: 1 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 7 | CDR Count | : 12 |
| Total WFA | : 0 | | |
| Transport-profile : R8-3 | | | |
| Redirection Requests | Rx: 0 | Redirection Responses | Tx: 0 |
| DRT Responses | Rx: 0 | DRT Requests | Tx: 1 |
| DRT successful Responses | Rx: 0 | DRT Error Responses | Rx: 0 |
| DRT Requests timed out | : 1 | CGF Switch Back Times | : 2 |
| Batch Requests | Tx: 1 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 7 | CDR Count | : 10 |
| Total WFA | : 1 | | |
| Transport-profile : R8-1 | | | |
| Redirection Requests | Rx: 0 | Redirection Responses | Tx: 0 |
| DRT Responses | Rx: 0 | DRT Requests | Tx: 1 |

| | | | |
|--------------------------|-------|-----------------------|-------|
| DRT successful Responses | Rx: 0 | DRT Error Responses | Rx: 0 |
| DRT Requests timed out | : 1 | CGF Switch Back Times | : 2 |
| Batch Requests | Tx: 1 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 7 | CDR Count | : 11 |
| Total WFA | : 1 | | |

Transport-profile : R7-1

| | | | |
|--------------------------|-------|-----------------------|-------|
| 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 | : 1 |
| Batch Requests | Tx: 1 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 7 | CDR Count | : 7 |
| Total WFA | : 1 | | |

Transport-profile : R99-1

| | | | |
|--------------------------|-------|-----------------------|-------|
| 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 | : 1 |
| Batch Requests | Tx: 1 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 7 | CDR Count | : 7 |
| Total WFA | : 1 | | |

Transport-profile : R7-2

| | | | |
|--------------------------|-------|-----------------------|-------|
| Redirection Requests | Rx: 0 | Redirection Responses | Tx: 0 |
| DRT Responses | Rx: 0 | DRT Requests | Tx: 1 |
| DRT successful Responses | Rx: 0 | DRT Error Responses | Rx: 0 |
| DRT Requests timed out | : 10 | CGF Switch Back Times | : 2 |
| Batch Requests | Tx: 1 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 7 | CDR Count | : 12 |
| Total WFA | : 1 | | |

Transport-profile : R8-2

| | | | |
|--------------------------|-------|-----------------------|-------|
| Redirection Requests | Rx: 0 | Redirection Responses | Tx: 0 |
| DRT Responses | Rx: 0 | DRT Requests | Tx: 1 |
| DRT successful Responses | Rx: 0 | DRT Error Responses | Rx: 0 |
| DRT Requests timed out | : 1 | CGF Switch Back Times | : 2 |
| Batch Requests | Tx: 1 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 7 | CDR Count | : 10 |
| Total WFA | : 1 | | |

FPC/PIC: 7/0

Transport-profile : R7-3

| | | | |
|--------------------------|-------|-----------------------|-------|
| 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 | | |

Transport-profile : R99-2

| | | | |
|--------------------------|-------|-----------------------|-------|
| 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 | | |

```

Transport-profile : R8-3
  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

```

```

Transport-profile : R8-1
  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

```

```

Transport-profile : R7-1
  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

```

```

Transport-profile : R99-1
  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

```

```

Transport-profile : R7-2
  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

```

```

Transport-profile : R8-2
  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: 7/1

```

Transport-profile : R7-3
  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 | | |
| Transport-profile : R99-2 | | | |
| 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 | | |
| Transport-profile : R8-3 | | | |
| 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 | | |
| Transport-profile : R8-1 | | | |
| 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 | | |
| Transport-profile : R7-1 | | | |
| 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 | | |
| Transport-profile : R99-1 | | | |
| 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 | | |
| Transport-profile : R7-2 | | | |
| 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 | | |
| Transport-profile : R8-2 | | | |
| 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: 9/0

Transport-profile : R7-3

| | | | |
|--------------------------|-------|-----------------------|-------|
| 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 | : 4 |
| Batch Requests | Tx: 0 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 0 | CDR Count | : 0 |
| Total WFA | : 0 | | |

Transport-profile : R99-2

| | | | |
|--------------------------|-------|-----------------------|-------|
| 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 | : 1 |
| Batch Requests | Tx: 0 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 0 | CDR Count | : 0 |
| Total WFA | : 0 | | |

Transport-profile : R8-3

| | | | |
|--------------------------|-------|-----------------------|-------|
| 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 | : 1 |
| Batch Requests | Tx: 0 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 0 | CDR Count | : 0 |
| Total WFA | : 0 | | |

Transport-profile : R8-1

| | | | |
|--------------------------|-------|-----------------------|-------|
| 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 | : 1 |
| Batch Requests | Tx: 0 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 0 | CDR Count | : 0 |
| Total WFA | : 0 | | |

Transport-profile : R7-1

| | | | |
|--------------------------|-------|-----------------------|-------|
| 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 | : 1 |
| Batch Requests | Tx: 0 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 0 | CDR Count | : 0 |
| Total WFA | : 0 | | |

Transport-profile : R99-1

| | | | |
|--------------------------|-------|-----------------------|-------|
| 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 | : 1 |
| Batch Requests | Tx: 0 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 0 | CDR Count | : 0 |
| Total WFA | : 0 | | |

Transport-profile : R7-2

| | | | |
|--------------------------|-------|-----------------------|-------|
| 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 | : 4 |
| Batch Requests | Tx: 0 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 0 | CDR Count | : 0 |
| Total WFA | : 0 | | |

Transport-profile : R8-2

| | | | |
|--------------------------|-------|-----------------------|-------|
| 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 | : 1 |
| Batch Requests | Tx: 0 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 0 | CDR Count | : 0 |
| Total WFA | : 0 | | |

FPC/PIC: 9/1

Transport-profile : R7-3

| | | | |
|--------------------------|-------|-----------------------|-------|
| Redirection Requests | Rx: 0 | 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 | : 29 | CGF Switch Back Times | : 4 |
| Batch Requests | Tx: 0 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 0 | CDR Count | : 10 |
| Total WFA | : 1 | | |

Transport-profile : R99-2

| | | | |
|--------------------------|-------|-----------------------|-------|
| 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 | : 1 |
| Batch Requests | Tx: 0 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 0 | CDR Count | : 0 |
| Total WFA | : 0 | | |

Transport-profile : R8-3

| | | | |
|--------------------------|-------|-----------------------|-------|
| 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 | : 1 |
| Batch Requests | Tx: 0 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 0 | CDR Count | : 0 |
| Total WFA | : 0 | | |

Transport-profile : R8-1

| | | | |
|--------------------------|--------|-----------------------|-------|
| 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 | : 1 |
| Batch Requests | Tx: 1 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 31 | CDR Count | : 31 |
| Total WFA | : 1 | | |

Transport-profile : R7-1

| | | | |
|--------------------------|-------|-----------------------|--------|
| Redirection Requests | Rx: 0 | Redirection Responses | Tx: 0 |
| DRT Responses | Rx: 0 | DRT Requests | Tx: 10 |
| DRT successful Responses | Rx: 0 | DRT Error Responses | Rx: 0 |
| DRT Requests timed out | : 27 | CGF Switch Back Times | : 5 |
| Batch Requests | Tx: 0 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 0 | CDR Count | : 60 |

Total WFA : 0

Transport-profile : R99-1

| | | | |
|--------------------------|-------|-----------------------|-------|
| 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 | : 1 |
| Batch Requests | Tx: 0 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 0 | CDR Count | : 0 |
| Total WFA | : 0 | | |

Transport-profile : R7-2

| | | | |
|--------------------------|-------|-----------------------|--------|
| Redirection Requests | Rx: 0 | Redirection Responses | Tx: 0 |
| DRT Responses | Rx: 0 | DRT Requests | Tx: 18 |
| DRT successful Responses | Rx: 0 | DRT Error Responses | Rx: 0 |
| DRT Requests timed out | : 223 | CGF Switch Back Times | : 6 |
| Batch Requests | Tx: 0 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 0 | CDR Count | : 90 |
| Total WFA | : 1 | | |

Transport-profile : R8-2

| | | | |
|--------------------------|-------|-----------------------|-------|
| 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 | : 1 |
| Batch Requests | Tx: 0 | Batch Response Errors | Rx: 0 |
| Batch CDR's | Tx: 0 | CDR Count | : 0 |
| Total WFA | : 0 | | |

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> <transport-profile-name profile-name></pre> |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Display the CDR transfer status for the configured transport profiles. |
| Options | <p>none—(Same as brief) Display the total number of unacknowledged and buffered CDRs for the configured transport profiles.</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 for the specified FPC slot number and PIC slot number only.</p> <p>transport-profile-name profile-name—(Optional) Display the total number of unacknowledged and buffered CDRs for the specified transport profile only.</p> |
| Required Privilege Level | view |
| List of Sample Output | show unified-edge ggsn-pgw charging transfer status on page 947 show unified-edge ggsn-pgw charging transfer status detail on page 947 |
| Output Fields | Table 70 on page 946 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. |

Table 70: show unified-edge ggsn-pgw charging transfer status Output Fields

| Field Name | Field Description | Level of Output |
|-----------------------------|---|--------------------|
| 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 (transport profile-wise) sent to the storage device (CGF servers or RE disk, or both) for which no acknowledgements were received from the storage device. | All levels none |
| Total Buffered CDR's | Total number of buffered CDRs in Service PICs for the configured transport profiles. | All levels none |
| FPC/PIC | FPC slot number/PIC slot number. | detail |

Sample Output

```

show unified-edge      user@host> show unified-edge ggsn-pgw charging transfer status
ggsn-pgw charging      Charging Transfer Status
transfer status        Transport-Profile : R7-1
                          Total UnAck CDR's       : 28
                          Total Buffered CDR's     : 129033

                          Transport-Profile : R7-2
                          Total UnAck CDR's       : 21
                          Total Buffered CDR's     : 14020

                          Transport-Profile : R7-3
                          Total UnAck CDR's       : 0
                          Total Buffered CDR's     : 3675

                          Transport-Profile : R8-1
                          Total UnAck CDR's       : 52
                          Total Buffered CDR's     : 178987

                          Transport-Profile : R8-2
                          Total UnAck CDR's       : 7
                          Total Buffered CDR's     : 239554

                          Transport-Profile : R8-3
                          Total UnAck CDR's       : 0
                          Total Buffered CDR's     : 4612

                          Transport-Profile : R99-1
                          Total UnAck CDR's       : 14
                          Total Buffered CDR's     : 135553

                          Transport-Profile : R99-2
                          Total UnAck CDR's       : 7
                          Total Buffered CDR's     : 179852


show unified-edge      user@host> show unified-edge ggsn-pgw charging transfer status detail
ggsn-pgw charging      Charging Transfer Status
transfer status detail FPC/PIC: 10/0
                          Transport-profile       : R7-3
                          Transport-profile Id     : 3
                          Total UnAck CDR's       : 0
                          Total Buffered CDR's     : 120

                          Transport-profile       : R99-2
                          Transport-profile Id     : 8
                          Total UnAck CDR's       : 7
                          Total Buffered CDR's     : 34126

                          Transport-profile       : R8-3
                          Transport-profile Id     : 6
                          Total UnAck CDR's       : 0
                          Total Buffered CDR's     : 135

                          Transport-profile       : R8-1
                          Transport-profile Id     : 4
                          Total UnAck CDR's       : 21
                          Total Buffered CDR's     : 41688

                          Transport-profile       : R7-1

```

Transport-profile Id : 1
Total UnAck CDR's : 28
Total Buffered CDR's : 47897

Transport-profile : R99-1
Transport-profile Id : 7
Total UnAck CDR's : 14
Total Buffered CDR's : 35019

Transport-profile : R7-2
Transport-profile Id : 2
Total UnAck CDR's : 21
Total Buffered CDR's : 1606

Transport-profile : R8-2
Transport-profile Id : 5
Total UnAck CDR's : 7
Total Buffered CDR's : 65815

FPC/PIC: 10/1
Transport-profile : R7-3
Transport-profile Id : 3
Total UnAck CDR's : 0
Total Buffered CDR's : 1760

Transport-profile : R99-2
Transport-profile Id : 8
Total UnAck CDR's : 0
Total Buffered CDR's : 71292

Transport-profile : R8-3
Transport-profile Id : 6
Total UnAck CDR's : 0
Total Buffered CDR's : 2125

Transport-profile : R8-1
Transport-profile Id : 4
Total UnAck CDR's : 0
Total Buffered CDR's : 34116

Transport-profile : R7-1
Transport-profile Id : 1
Total UnAck CDR's : 0
Total Buffered CDR's : 1018

Transport-profile : R99-1
Transport-profile Id : 7
Total UnAck CDR's : 0
Total Buffered CDR's : 1574

Transport-profile : R7-2
Transport-profile Id : 2
Total UnAck CDR's : 0
Total Buffered CDR's : 159

Transport-profile : R8-2
Transport-profile Id : 5
Total UnAck CDR's : 0
Total Buffered CDR's : 336

FPC/PIC: 7/0

| | |
|----------------------|---------|
| Transport-profile | : R7-3 |
| Transport-profile Id | : 3 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 0 |
| Transport-profile | : R99-2 |
| Transport-profile Id | : 8 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 0 |
| Transport-profile | : R8-3 |
| Transport-profile Id | : 6 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 0 |
| Transport-profile | : R8-1 |
| Transport-profile Id | : 4 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 0 |
| Transport-profile | : R7-1 |
| Transport-profile Id | : 1 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 0 |
| Transport-profile | : R99-1 |
| Transport-profile Id | : 7 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 0 |
| Transport-profile | : R7-2 |
| Transport-profile Id | : 2 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 0 |
| Transport-profile | : R8-2 |
| Transport-profile Id | : 5 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 0 |
| FPC/PIC: 7/1 | |
| Transport-profile | : R7-3 |
| Transport-profile Id | : 3 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 461 |
| Transport-profile | : R99-2 |
| Transport-profile Id | : 8 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 0 |
| Transport-profile | : R8-3 |
| Transport-profile Id | : 6 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 431 |
| Transport-profile | : R8-1 |
| Transport-profile Id | : 4 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 8827 |

| | |
|----------------------|---------|
| Transport-profile | : R7-1 |
| Transport-profile Id | : 1 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 8852 |
| Transport-profile | : R99-1 |
| Transport-profile Id | : 7 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 9685 |
| Transport-profile | : R7-2 |
| Transport-profile Id | : 2 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 4377 |
| Transport-profile | : R8-2 |
| Transport-profile Id | : 5 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 0 |
| FPC/PIC: 8/0 | |
| Transport-profile | : R7-3 |
| Transport-profile Id | : 3 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 80 |
| Transport-profile | : R99-2 |
| Transport-profile Id | : 8 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 32584 |
| Transport-profile | : R8-3 |
| Transport-profile Id | : 6 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 90 |
| Transport-profile | : R8-1 |
| Transport-profile Id | : 4 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 39899 |
| Transport-profile | : R7-1 |
| Transport-profile Id | : 1 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 45932 |
| Transport-profile | : R99-1 |
| Transport-profile Id | : 7 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 33537 |
| Transport-profile | : R7-2 |
| Transport-profile Id | : 2 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 1566 |
| Transport-profile | : R8-2 |
| Transport-profile Id | : 5 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 62830 |

```
FPC/PIC: 8/1
Transport-profile      : R7-3
Transport-profile Id   : 3
Total UnAck CDR's     : 0
Total Buffered CDR's   : 869

Transport-profile      : R99-2
Transport-profile Id   : 8
Total UnAck CDR's     : 0
Total Buffered CDR's   : 66672

Transport-profile      : R8-3
Transport-profile Id   : 6
Total UnAck CDR's     : 0
Total Buffered CDR's   : 1486

Transport-profile      : R8-1
Transport-profile Id   : 4
Total UnAck CDR's     : 0
Total Buffered CDR's   : 75607

Transport-profile      : R7-1
Transport-profile Id   : 1
Total UnAck CDR's     : 0
Total Buffered CDR's   : 50806

Transport-profile      : R99-1
Transport-profile Id   : 7
Total UnAck CDR's     : 0
Total Buffered CDR's   : 71204

Transport-profile      : R7-2
Transport-profile Id   : 2
Total UnAck CDR's     : 0
Total Buffered CDR's   : 2943

Transport-profile      : R8-2
Transport-profile Id   : 5
Total UnAck CDR's     : 0
Total Buffered CDR's   : 158431

FPC/PIC: 9/0
Transport-profile      : R7-3
Transport-profile Id   : 3
Total UnAck CDR's     : 0
Total Buffered CDR's   : 0

Transport-profile      : R99-2
Transport-profile Id   : 8
Total UnAck CDR's     : 0
Total Buffered CDR's   : 0

Transport-profile      : R8-3
Transport-profile Id   : 6
Total UnAck CDR's     : 0
Total Buffered CDR's   : 0

Transport-profile      : R8-1
Transport-profile Id   : 4
Total UnAck CDR's     : 0
Total Buffered CDR's   : 0
```

| | |
|----------------------|---------|
| Transport-profile | : R7-1 |
| Transport-profile Id | : 1 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 0 |
| Transport-profile | : R99-1 |
| Transport-profile Id | : 7 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 0 |
| Transport-profile | : R7-2 |
| Transport-profile Id | : 2 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 0 |
| Transport-profile | : R8-2 |
| Transport-profile Id | : 5 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 0 |
| FPC/PIC: 9/1 | |
| Transport-profile | : R7-3 |
| Transport-profile Id | : 3 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 468 |
| Transport-profile | : R99-2 |
| Transport-profile Id | : 8 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 0 |
| Transport-profile | : R8-3 |
| Transport-profile Id | : 6 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 438 |
| Transport-profile | : R8-1 |
| Transport-profile Id | : 4 |
| Total UnAck CDR's | : 31 |
| Total Buffered CDR's | : 8971 |
| Transport-profile | : R7-1 |
| Transport-profile Id | : 1 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 8972 |
| Transport-profile | : R99-1 |
| Transport-profile Id | : 7 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 9821 |
| Transport-profile | : R7-2 |
| Transport-profile Id | : 2 |
| Total UnAck CDR's | : 0 |
| Total Buffered CDR's | : 4439 |
| Transport-profile | : R8-2 |
| Transport-profile Id | : 5 |
| 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. |
| 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 for the specified trigger profile only.</p> |
| Required Privilege Level | view |
| List of Sample Output | show unified-edge ggsn-pgw charging trigger-profile on page 955 |
| Output Fields | Table 71 on page 954 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 71: 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 |
| PLMN change trigger | Whether the PLMN change trigger is enabled. | All levels |
| | If this trigger is enabled, a PLMN change usually results in the CDR getting updated with the charging information and the CDR getting closed. | none |
| QoS change trigger | Whether the QoS change trigger is enabled. | All levels |
| | If this trigger is enabled, a QoS change usually results in a container getting added to the CDR. | none |
| RAT change trigger | Whether the RAT change trigger is enabled. | All levels |
| | If this trigger is enabled, a RAT change usually results in the CDR getting updated with the charging information and the CDR getting closed. | none |
| User location change trigger | Whether the user-location change trigger is enabled. | All levels |
| | If this trigger is enabled, a user location change usually results in the open containers getting closed and added to the CDR. | none |

Table 71: show unified-edge ggsn-pgw charging trigger-profile Output Fields (*continued*)

| Field Name | Field Description | Level of Output |
|-----------------------------------|---|-----------------|
| MS Timezone change trigger | Whether the MS time zone change trigger is enabled. | All levels |
| | If this trigger is enabled, an MS time zone change usually results in the CDR getting updated with the charging information and the CDR getting closed. | none |

Sample Output

```

show unified-edge ggsn-pgw charging trigger-profile user@host> show unified-edge ggsn-pgw charging trigger-profile
Profile Name: __default_trigger_profile__
Profile ID : 0
PLMN change trigger: Enabled
QOS change trigger : Enabled
RAT change trigger : Enabled
User location change trigger: Enabled
MS Timezone change trigger: Enabled

Profile Name: tp1
Profile ID : 1
PLMN change trigger: Enabled
QOS change trigger : Enabled
RAT change trigger : Enabled
User location change trigger: Enabled
MS Timezone change trigger: Enabled

Profile Name: tp2
Profile ID : 2
PLMN change trigger: Enabled
QOS change trigger : Enabled
RAT 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 <arp> <gateway> <gtpv1-arp> <qci> <traffic-class> <traffic-handling-priority> |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | Display standard information about the results of the ggsn-pgw qos statistics status. |
| Options | arp—Display the allocation and retention priority (ARP). gateway—Display the subscriber information from the specified gateway. gtpv1-arp—Display information for the GTPv1 ARP. QCI—Display the QCI statistics information. traffic-class—Displays the statistics for a traffic-class level. traffic-handling-priority—Display information for the traffic handling priority. |
| Required Privilege Level | view |
| List of Sample Output | show unified-edge ggsn-pgw qos statistics on page 959 |
| Output Fields | Table 72 on page 958 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 72: show unified-edge ggsn-pgw qos statistics Output Fields

| Field Name | Field Description |
|---|--|
| Control plane statistics | Display information about the control plane statistics such as session-establishment-attempts, peer-initiated-sessions, and gateway-initiated-session-deactivations. |
| Data plane GTP statistics (Gn/S5/S8) | Display information about the data plane GTP statistics such as input and output packets and bytes and discarded packets for Gn, S5, and S8. |
| Data plane GTP statistics (Gi) | Display information about the data plane GTP statistics such as input and output packets and bytes and discarded packets for Gi. |

Sample Output

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

show unified-edge ggsn-pgw status preemption-list

Syntax `show unified-edge ggsn-pgw status preemption-list`
`<brief | detail>`
`<fpc-slot fpc-slot>`
`<pic-slot pic-slot>`

Release Information Command introduced in Junos OS Mobility Release 11.2W.

Description Display the preemption list for guaranteed bit rate (GBR) and non-GBR bearers in the broadband gateway.



NOTE: In load conditions, to accommodate higher-priority bearers, lower-priority bearers will be preempted. This list displays the number of bearers in each candidate priority level for preemption.

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.

`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 ggsn-pgw status on page 862](#)

List of Sample Output [show unified-edge ggsn-pgw status preemption-list on page 961](#)
[show unified-edge ggsn-pgw status preemption-list detail on page 961](#)

Output Fields [Table 73 on page 960](#) 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 73: show unified-edge ggsn-pgw status preemption-list Output Fields

| Field Name | Field Description | Level of Output |
|------------|--|-----------------|
| 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 |

Table 73: show unified-edge ggsn-pgw status preemption-list Output Fields (*continued*)

| Field Name | Field Description | Level of Output |
|----------------|--|-----------------|
| 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
user@host> show unified-edge ggsn-pgw status preemption-list
                                     GBR      NON-GBR
Priority Level 1      :      0      20000
Priority Level 2      :      0      0
Priority Level 3      :      0      0
Priority Level 4      :      0      1000
Priority Level 5      :      0      0
Priority Level 6      :      0      19981
Priority Level 7      :      0      0
Priority Level 8      :      0      6128
Priority Level 9      :      0      0
Priority Level 10     :      0      0
Priority Level 11     :      0      2731
Priority Level 12     :      0      17362
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
Preemption List status:
FPC SLOT: 1   PIC SLOT: 0

                                     GBR      NON-GBR
Priority Level 1      :      0      9997
Priority Level 2      :      0      0
Priority Level 3      :      0      0
Priority Level 4      :      0      508
Priority Level 5      :      0      0
Priority Level 6      :      0      9992
Priority Level 7      :      0      0
Priority Level 8      :      0      2994
Priority Level 9      :      0      0
Priority Level 10     :      0      0
Priority Level 11     :      0      1303
Priority Level 12     :      0      8819
Priority Level 13     :      0      0
Priority Level 14     :      0      0
Priority Level 15     :      0      0

Preemption List status:
FPC SLOT: 1   PIC SLOT: 1

                                     GBR      NON-GBR

```

| | | | |
|-------------------|---|---|-------|
| Priority Level 1 | : | 0 | 10003 |
| Priority Level 2 | : | 0 | 0 |
| Priority Level 3 | : | 0 | 0 |
| Priority Level 4 | : | 0 | 492 |
| Priority Level 5 | : | 0 | 0 |
| Priority Level 6 | : | 0 | 9989 |
| Priority Level 7 | : | 0 | 0 |
| Priority Level 8 | : | 0 | 3134 |
| Priority Level 9 | : | 0 | 0 |
| Priority Level 10 | : | 0 | 0 |
| Priority Level 11 | : | 0 | 1428 |
| Priority Level 12 | : | 0 | 8543 |
| 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 exception-handling statistics

| | |
|---------------------------------|---|
| Syntax | <code>clear unified-edge ggsn-pgw exception-handling statistics</code> <code><error-indication failover invalid-subscriber></code> <code><fpc-slot <i>fpc-slot</i>></code> <code><inet></code> <code><pic-slot <i>pic-slot</i>></code> |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Clear the exception handling statistics per services PIC. If the services PIC slot is not specified, then the statistics for all services PICs are cleared. |
| Options | <p><code>none</code>—Clear the exception handling statistics for all services PICs.</p> <p><code>error-indication</code>—(Optional) Clear the error indication statistics.</p> <p><code>failover</code>—(Optional) Clear the anchor Packet Forwarding Engine failover statistics.</p> <p><code>fpc-slot <i>fpc-slot</i></code>—(Optional) Clear the exception handling statistics for the specified Flexible PIC Concentrator (FPC).</p> <p><code>inet</code>—(Optional) Clear the exception handling statistics for IPv4 packets.</p> <p><code>invalid-subscriber</code>—(Optional) Clear the invalid subscriber statistics.</p> <p><code>pic-slot <i>pic-slot</i></code>—(Optional) Clear the exception handling 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 exception-handling statistics on page 966 |
| List of Sample Output | clear unified-edge ggsn-pgw exception-handling statistics fpc-slot 5 pic-slot 0 on page 964 |
| 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 exception-handling statistics fpc-slot 5 pic-slot 0</code> | <code>user@host> clear unified-edge ggsn-pgw exception-handling statistics fpc-slot 5 pic-slot 0</code> Invalid subscriber statistics cleared for FPC 5 PIC 0 Failover statistics cleared for FPC 5 PIC 0 Error Indication statistics cleared for FPC 5 PIC 0 |
|--|---|

clear unified-edge ggsn-pgw ip-reassembly statistics

| | |
|---------------------------------|---|
| Syntax | clear unified-edge ggsn-pgw ip-reassembly statistics <fpc-slot <i>fpc-slot</i> > <inet> <pic-slot <i>pic-slot</i> > |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Clear the IP reassembly statistics per services PIC. If the services PIC slot is not specified, then the statistics for all the services PICs are cleared. |
| Options | <p>none—Clear the IP reassembly statistics for all services PICs.</p> <p>fpc-slot <i>fpc-slot</i>—(Optional) Clear the IP reassembly statistics for the specified Flexible PIC Concentrator (FPC).</p> <p>inet—(Optional) Clear the IP reassembly for IPv4 packets.</p> <p>pic-slot <i>pic-slot</i>—(Optional) Clear the IP reassembly 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 ip-reassembly statistics on page 970 |
| List of Sample Output | clear unified-edge ggsn-pgw ip-reassembly statistics fpc-slot 5 pic-slot 0 on page 965 |
| 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 ip-reassembly statistics fpc-slot 5 pic-slot 0
ggsn-pgw           IP reassembly statistics cleared for FPC 5 PIC 0
ip-reassembly
statistics fpc-slot 5
pic-slot 0

```

show unified-edge ggsn-pgw exception-handling statistics

Syntax `show unified-edge ggsn-pgw exception-handling statistics`
`<brief | detail>`
`<error-indication | failover | invalid-subscriber>`
`<fpc-slot fpc-slot>`
`<pic-slot pic-slot>`

Release Information Command introduced in Junos OS Mobility Release 11.2W.

Description Display the exception handling statistics per services PIC. If the services PIC slot is not specified, then the statistics for all services PICs are displayed.

Options none—(Same as brief) Display the exception handling statistics in brief.
 brief | detail—(Optional) Display the specified level of output.



NOTE: The **brief** option displays the aggregated statistics from each services PIC. The **detail** option displays statistics for each services PIC separately.

error-indication—(Optional) Display the error indication statistics only for transmitted packets.

failover—(Optional) Display the anchor Packet Forwarding Engine failover statistics.

invalid-subscriber—(Optional) Display the invalid subscriber statistics.

fpc-slot *fpc-slot*—(Optional) Display the exception handling statistics for the specified Flexible PIC Concentrator (FPC) slot number.

pic-slot *pic-slot*—(Optional) Display the exception handling 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 • [clear unified-edge ggsn-pgw exception-handling statistics on page 964](#)

List of Sample Output [show unified-edge ggsn-pgw exception-handling statistics brief on page 967](#)
[show unified-edge ggsn-pgw exception-handling statistics detail on page 968](#)

Output Fields [Table 74 on page 967](#) lists the output fields for the **show unified-edge ggsn-pgw exception-handling statistics** command. Output fields are listed in the approximate order in which they appear.

Table 74: show unified-edge ggsn-pgw exception-handling statistics Output Fields

| Field Name | Field Description | Level of Output |
|--|--|-----------------|
| FPC Slot | FPC slot number for which the corresponding statistics are displayed. | detail |
| PIC slot | PIC slot number for which the corresponding statistics are displayed. | detail |
| Invalid subscriber statistics | <p>Statistics for invalid subscribers for GTPv0 Uplink, GTPv1 Uplink, Inet Downlink, and Inet6 Downlink:</p> <ul style="list-style-type: none"> • Total Packets received—Total number of packets pertaining to invalid subscribers received from the Packet Forwarding Engine • Invalid Packets—Number of packets pertaining to invalid subscribers and that failed the validation checks; these packets are received from the Packet Forwarding Engine. • Flows created—Number of flows created to handle packets pertaining to invalid subscribers. • Flows aged out—Number of flows aged out. | All levels |
| Anchor PFE failover statistics: | <p>Anchor Packet Forwarding Engine failover statistics for GTPv0 Uplink, GTPv1 Uplink, Inet Downlink, and Inet6 Downlink:</p> <ul style="list-style-type: none"> • Reprogram triggers—Number of times the system triggered the expedited reprogramming of subscribers. | All levels |
| Error indication statistics | <p>Error indication statistics for GTPv0 Uplink and GTPv1 Uplink:</p> <ul style="list-style-type: none"> • Error indications sent—Number of error indications successfully sent. • Error indications send failures—Number of error indications that could not be sent. | All levels |

Sample Output

```

show unified-edge ggsn-pgw exception-handling statistics brief
user@host> show unified-edge ggsn-pgw exception-handling statistics brief
Invalid subscriber statistics:
GTPv0 Uplink:
  Total Packets received:      1
  Invalid packets:            0
  Flows created:               1
  Flows aged out:             1
GTPv1 Uplink:
  Total Packets received:      1
  Invalid packets:            0
  Flows created:               1
  Flows aged out:             1
Inet Downlink:
  Total Packets received:      0
  Invalid packets:            0
  Flows created:               0
  Flows aged out:             0
Inet6 Downlink:
  Total Packets received:      0
  Invalid packets:            0
  Flows created:               0
  Flows aged out:             0

```

```
Anchor PFE failover statistics:
GTPv0 Uplink:
  Reprogram triggers:          0
GTPv1 Uplink:
  Reprogram triggers:          0
Inet Downlink:
  Reprogram triggers:          0
Inet6 Downlink:
  Reprogram triggers:          0
```

```
Error indication statistics:
GTPv0 Uplink:
  Error indications sent:       1
  Error indications send failures: 0
GTPv1 Uplink:
  Error indications sent:       1
  Error indications send failures: 0
```

```
show unified-edge ggsn-pgw exception-handling statistics detail
user@host> show unified-edge ggsn-pgw exception-handling statistics detail
```

```
Invalid subscriber statistics (FPC 5 PIC 1):
GTPv0 Uplink:
  Total Packets received:       0
  Invalid packets:              0
  Flows created:                0
  Flows aged out:               0
GTPv1 Uplink:
  Total Packets received:       1
  Invalid packets:              0
  Flows created:                1
  Flows aged out:               1
Inet Downlink:
  Total Packets received:       0
  Invalid packets:              0
  Flows created:                0
  Flows aged out:               0
Inet6 Downlink:
  Total Packets received:       0
  Invalid packets:              0
  Flows created:                0
  Flows aged out:               0
```

```
Anchor PFE failover statistics (FPC 5 PIC 1):
GTPv0 Uplink:
  Reprogram triggers:          0
GTPv1 Uplink:
  Reprogram triggers:          0
Inet Downlink:
  Reprogram triggers:          0
Inet6 Downlink:
  Reprogram triggers:          0
```

```
Error indication statistics (FPC 5 PIC 1):
GTPv0 Uplink:
  Error indications sent:       0
```



```
Error indications send failed: 0
GTPv1 Uplink:
Error indications sent: 1
Error indications send failed: 0
```

Invalid subscriber statistics (FPC 5 PIC 0):

```
GTPv0 Uplink:
Total Packets received: 1
Invalid packets: 0
Flows created: 1
Flows aged out: 1
GTPv1 Uplink:
Total Packets received: 0
Invalid packets: 0
Flows created: 0
Flows aged out: 0
Inet Downlink:
Total Packets received: 0
Invalid packets: 0
Flows created: 0
Flows aged out: 0
Inet6 Downlink:
Total Packets received: 0
Invalid packets: 0
Flows created: 0
Flows aged out: 0
```

Anchor PFE failover statistics (FPC 5 PIC 0):

```
GTPv0 Uplink:
Reprogram triggers: 0
GTPv1 Uplink:
Reprogram triggers: 0
Inet Downlink:
Reprogram triggers: 0
Inet6 Downlink:
Reprogram triggers: 0
```

Error indication statistics (FPC 5 PIC 0):

```
GTPv0 Uplink:
Error indications sent: 1
Error indications send failed: 0
GTPv1 Uplink:
Error indications sent: 0
Error indications send failed: 0
```

show unified-edge ggsn-pgw ip-reassembly statistics

Syntax `show unified-edge ggsn-pgw ip-reassembly statistics`
`<brief | detail>`
`<fpc-slot fpc-slot>`
`<inet>`
`<pic-slot pic-slot>`

Release Information Command introduced in Junos OS Mobility Release 11.2W.

Description Display the IP reassembly statistics per services PIC. If the services PIC slot is not specified, then the statistics for all the services PICs are displayed.

Options none—(Same as brief) Display the IP reassembly statistics in brief.
 brief | detail—(Optional) Display the specified level of output.



NOTE: The brief option displays the aggregated statistics from each services PIC.

`fpc-slot fpc-slot`—(Optional) Display the IP reassembly statistics for the specified Flexible PIC Concentrator (FPC) slot number.

`inet`—(Optional) Display the IP reassembly for IPv4 packets.

`pic-slot pic-slot`—(Optional) Display the IP reassembly 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 • [clear unified-edge ggsn-pgw ip-reassembly statistics on page 965](#)

List of Sample Output [show unified-edge ggsn-pgw ip-reassembly statistics brief on page 971](#)
[show unified-edge ggsn-pgw ip-reassembly statistics detail on page 972](#)

Output Fields [Table 75 on page 970](#) 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.

Table 75: show unified-edge ggsn-pgw ip-reassembly statistics Output Fields

| Field Name | Field Description | Level of Output |
|--------------------------|---|-----------------|
| IP Reassembly Statistics | | |
| FPC Slot | FPC slot number for which the statistics are displayed. | detail |

Table 75: show unified-edge ggsn-pgw ip-reassembly statistics Output Fields (*continued*)

| Field Name | Field Description | Level of Output |
|--------------------------------|--|-----------------|
| 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 ggsn-pgw ip-reassembly statistics brief
user@host> show unified-edge ggsn-pgw ip-reassembly statistics brief
IP reassembly statistics:
  First fragments:      1947359
  Non-first fragments:  1940342
  Total fragments:     3887701

```

```
Reassembled packets:      1836763
Merged packets:           0
Packets pending reassembly: 0
Timed out packets:        1000
Timed out fragments:      1000
Exceeded maximum packet length:1836763
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 IP reassembly statistics (FPC 3 PIC 0):
ip-reassembly First fragments:      1947359
statistics detail Non-first fragments: 1940342
Total fragments: 3887701
Reassembled packets: 1836763
Merged packets: 0
Packets pending reassembly: 0
Timed out packets: 1000
Timed out fragments: 1000
Exceeded maximum packet length:1836763
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

show unified-edge ggsn-pgw gtp statistics

| | |
|---------------------------------|--|
| Syntax | show unified-edge ggsn-pgw gtp statistics <fpc-slot <i>slot</i> > <gateway> <gtp-all> <gtp-v0> <gtp-v1> <gtp-v2> <pic-slot <i>slot</i> > |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | Display standard information about the results of the service edge for a 3GPP GTP statistics. |
| Options | fpc-slot <i>slot</i> —Display statistics for a Flexible PIC Concentrator (FPC) slot. gateway—Display information for the GTP gateway. gtp-all—Display information for all of the GTPs. gtp-v0—Display information for the GTP version 0. gtp-v1—Display information for the GTP version 1. gtp-v2—Display information for the GTP version 2. pic-slotslot—Display information from the specified PIC slot. |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> • clear unified-edge ggsn-pgw gtp statistics on page 978 |
| List of Sample Output | show unified-edge ggsn-pgw gtp statistics on page 975 |
| Output Fields | Table 72 on page 884 lists the output fields for the show unified-edge ggsn-pgw gtp statistics command. Output fields are listed in the approximate order in which they appear. |

Table 76: show unified-edge ggsn-pgw gtp statistics Output Fields

| Field Name | Field Description |
|------------------------|---|
| Drop Counter | Number of packets dropped. |
| Packet Allocation Fail | Status of the failed packet authentication. |
| Packet Send Fail | Status of the failed packet delivery. |

Table 76: show unified-edge ggsn-pgw gtp statistics Output Fields (*continued*)

| Field Name | Field Description |
|---------------------------|---|
| IP Version Error Rx | Status of the packet delivery. |
| IP Protocol Error | Details of the IP protocol error. |
| GTP Port Error | Details of the GTP protocol error. |
| GTPv0 Error Indication Rx | Details of the GTPv0 error indications. |
| Unknown Msg Rx | Details of the unknown message. |
| Packet Length Error Rx | Details of the packet length error. |

Sample Output

```

show unified-edge user@host> show unified-edge ggsn-pgw gtp statistics
ggsn-pgw gtp
statistics
Drop Counter           : 0   Packet Allocation Fail : 0
Packet Send Fail       : 0   IP Version Error Rx    : 0
IP Protocol Error Rx   : 0   GTP Port Error Rx      : 0
Packet Length Error Rx : 0   Unknown Msg Rx         : 0
GTPv0 Error Indication Rx : 0 GTPv0 Error Indication Tx : 0
GTPv1 Error Indication Rx : 0 GTPv1 Error Indication Tx : 0

```

show unified-edge ggsn-pgw gtp peer

| | |
|---------------------------------|--|
| Syntax | show unified-edge ggsn-pgw gtp peer <fpc-slot <i>slot</i> > <local-address <i>address</i> > <pic-slot <i>slot</i> > <remote-address <i>address</i> > <routing-instance <i>name</i> > <statistics> |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | Display standard information about the results of the service edge for a 3GPP GTP peer group. |
| Options | <p>fpc-slot <i>slot</i>—Display statistics for a Flexible PIC Concentrator (FPC) slot.</p> <p>local-address <i>address</i>—Display information for the local address.</p> <p>pic-slot <i>slot</i>—Display information from the specified PIC slot.</p> <p>remote-address <i>address</i>—Display information for the specified address.</p> <p>routing-instance <i>name</i>—Display information for the routing instance.</p> <p>statistics—Display information for the statistics.</p> |
| Required Privilege Level | view |
| Related Documentation | <ul style="list-style-type: none"> • clear unified-edge ggsn-pgw gtp peer statistics on page 979 |
| List of Sample Output | show unified-edge ggsn-pgw gtp peer on page 976 |
| Output Fields | Table 73 on page 886 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 77: show unified-edge ggsn-pgw gtp statistics Output Fields

| Field Name | Field Description |
|------------------|--|
| Rmt IP Address | IP address of the remote system. |
| Local IP Address | Local address of the system. |
| Routing-Instance | Routing instance for the ping attempt. |

Sample Output

```
show unified-edge user@host> show unified-edge ggsn-pgw gtp peer
ggsn-pgw gtp peer
```


| Rmt IP Address | Local IP Address | Routing-Instance |
|----------------|------------------|------------------|
| 10.10.7.83 | 91.92.1.5 | 0 |
| 10.10.7.83 | 91.92.1.5 | 0 |

clear unified-edge ggsn-pgw gtp statistics

| | |
|---------------------------------|--|
| Syntax | clear unified-edge ggsn-pgw gtp statistics <fpc-slot <i>slot</i> > <gateway> <gtp-all> <gtp-v0> <gtp-v1> <gtp-v2> <pic-slot <i>slot</i> > |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | On MX Series routers, clear information and the links on the service edge for 3GPP GTP statistics. |
| Options | <p>fpc-slot <i>slot</i>—Clear information for the specified FPC slot.</p> <p>gateway—Clear statistics for a gateway.</p> <p>gtp-all—Clear information for all of the GTPs.</p> <p>gtp-v0—Clear information for the GTP version 0.</p> <p>gtp-v1—Clear information for the GTP version 1.</p> <p>gtp-v2—Clear information for the GTP version 2.</p> <p>pic-slot <i>slot</i>—Clear the specified 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 974 |

clear unified-edge ggsn-pgw gtp peer statistics

| | |
|---------------------------------|---|
| Syntax | <pre>clear unified-edge ggsn-pgw gtp peer statistics <fpc-slot slot> <gtp-all> <gtp-v0> <gtp-v1> <gtp-v2> <local-address address> <pic-slot slot> <remote-address address> <routing-instance name></pre> |
| Release Information | Statement introduced in Junos OS Mobility Release 11.2W. |
| Description | On MX Series routers, clear information and the links on the service edge for 3GPP GTP statistics. |
| Options | <p>fpc-slot <i>slot</i>—Clear the number for the specified FPC slot.</p> <p>gtp-all—Clear information for all of the GTPs.</p> <p>gtp-v0—Clear information for the GTP version 0.</p> <p>gtp-v1—Clear information for the GTP version 1.</p> <p>gtp-v2—Clear information for the GTP version 2.</p> <p>local-address <i>address</i>—Clear the local IP address information for the peer.</p> <p>pic-slot <i>slot</i>—Clear the specified PIC slot number.</p> <p>remote-address <i>address</i>—Clear the remote IP address information of the peer.</p> <p>routing-instance <i>instance</i>—Clear routing instance information of the peer.</p> |
| Required Privilege Level | clear |

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 984](#)
[show services flows count interface ams0 on page 985](#)

Output Fields [Table 78 on page 984](#) 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 78: show services flows Output Fields

| Field Name | Field Description | Level of Output |
|--------------------------|--|-------------------|
| Interface | Name of the interface. | 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-4/0/0, Service set: Src_static
Flow
TCP      150.10.10.129:39249 -> 160.10.10.2:21      Forward I      Frm count
TCP      160.10.10.2:21 -> 50.1.8.11:1092      Forward O      11
TCP      150.10.10.213:38676 -> 160.10.10.23:21     Forward I      10
TCP      160.10.10.23:21 -> 50.1.7.111:1089     Forward O      11
TCP      150.10.10.63:38570 -> 160.10.10.6:21      Forward I      10
TCP      160.10.10.6:21 -> 50.1.7.80:1087      Forward O      11
TCP      150.10.10.146:38040 -> 160.10.10.7:21      Forward I      10
TCP      160.10.10.7:21 -> 50.1.6.177:1088      Forward O      10

```



```

TCP      150.10.10.195:37791 -> 160.10.10.10:21 Forward I      11
TCP      160.10.10.10:21 -> 50.1.6.92:1091 Forward 0      10
TCP      150.10.10.98:37771 -> 160.10.10.3:21 Forward I      11
TCP      160.10.10.3:21 -> 50.1.6.83:1090 Forward 0      10
TCP      150.10.10.193:37717 -> 160.10.10.5:21 Forward I      11
TCP      160.10.10.5:21 -> 50.1.6.65:1089 Forward 0      10
TCP      150.10.10.10:37711 -> 160.10.10.20:554 Forward I      9
[...output truncated...]

```

Interface: mams-5/0/0, Service set: Src_static

| Flow | State | Dir | Frm count |
|--|---------|-----|-----------|
| TCP 150.10.10.64:12996 -> 160.10.10.97:21 | Forward | I | 11 |
| TCP 160.10.10.97:21 -> 50.1.99.124:1091 | Forward | O | 10 |
| TCP 150.10.10.86:12701 -> 160.10.10.29:21 | Forward | I | 11 |
| TCP 160.10.10.29:21 -> 50.1.99.36:1091 | Forward | O | 10 |
| TCP 150.10.10.22:12040 -> 160.10.10.28:21 | Forward | I | 11 |
| TCP 160.10.10.28:21 -> 50.1.98.76:1092 | Forward | O | 10 |
| TCP 150.10.10.149:11628 -> 160.10.10.34:21 | Forward | I | 11 |
| TCP 160.10.10.34:21 -> 50.1.97.194:1094 | Forward | O | 10 |
| TCP 150.10.10.104:11436 -> 160.10.10.24:21 | Forward | I | 11 |
| TCP 160.10.10.24:21 -> 50.1.97.124:1092 | Forward | O | 10 |
| TCP 150.10.10.50:11397 -> 160.10.10.11:21 | Forward | I | 11 |
| TCP 160.10.10.11:21 -> 50.1.97.111:1093 | Forward | O | 10 |
| TCP 150.10.10.81:11076 -> 160.10.10.4:21 | Forward | I | 11 |
| TCP 160.10.10.4:21 -> 50.1.96.246:1095 | Forward | O | 10 |

[...output truncated...]

**show services flows
count interface ams0**

user@host> show services flows count interface ams0

| Interface | Service set | Flow count |
|------------|-------------|------------|
| mams-4/0/0 | Src_static | 2158 |
| mams-4/1/0 | Src_static | 0 |
| mams-5/0/0 | Src_static | 1630 |

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 | <i>pool-name</i> —(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 eim on page 988 • show services nat mappings summary on page 990 |
| List of Sample Output | show services nat mappings app on page 987 |
| Output Fields | Table 79 on page 986 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 79: 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 | <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 app user@host> show services nat mappings app
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 | <i>pool-name</i> —(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 986 • show services nat mappings summary on page 990 |
| List of Sample Output | show services nat mappings eim on page 989 |
| Output Fields | Table 80 on page 988 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 80: 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 986• show services nat mappings eim on page 988 |
| List of Sample Output | show services nat mappings summary on page 990 |
| Output Fields | Table 81 on page 990 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 81: 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 992 show services nat pool detail (Aggregated Multiservices) on page 992 show services nat pool dynamic_pool detail on page 992 |
| Output Fields | Table 82 on page 991 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 82: show services nat pool Output Fields

| Field Name | Field Description | Level of Output |
|-----------------------------------|---|-----------------|
| Interface | Name of the aggregated multiservices member interface (mams-). | 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 |
| 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 |

Table 82: show services nat pool Output Fields (*continued*)

| Field Name | Field Description | Level of Output |
|---------------------------|--|-----------------|
| 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-4/0/0, Service set: Src_static
NAT pool      Type    Address                               Port    Ports used
pool1         NAPT-44 50.1.0.0-50.1.42.169                1024-65535 1266
                    50.1.127.254-50.1.127.255

Interface: mams-4/1/0, Service set: Src_static
NAT pool      Type    Address                               Port    Ports used
pool1         NAPT-44 50.1.42.170-50.1.85.83              1024-65535 270

Interface: mams-5/0/0, Service set: Src_static
NAT pool      Type    Address                               Port    Ports used
pool1         NAPT-44 50.1.85.84-50.1.127.253            1024-65535 959

user@host> show services nat pool detail
show services nat pool detail (Aggregated Multiservices)
Interface: mams-4/0/0, Service set: Src_static
NAT pool: pool1, Translation type: NAPT-44
Address range: 50.1.0.0-50.1.42.169
Address range: 50.1.127.254-50.1.127.255
Port range: 1024-65535, Ports in use: 1266, Out of port errors: 0, Max ports
used: 84880

Interface: mams-4/1/0, Service set: Src_static
NAT pool: pool1, Translation type: NAPT-44
Address range: 50.1.42.170-50.1.85.83
Port range: 1024-65535, Ports in use: 299, Out of port errors: 0, Max ports
used: 86189

Interface: mams-5/0/0, Service set: Src_static
NAT pool: pool1, Translation type: NAPT-44
Address range: 50.1.85.84-50.1.127.253
Port range: 1024-65535, Ports in use: 959, Out of port errors: 0, Max ports
used: 87933

user@host> show services nat pool dynamic_pool detail
show services nat pool dynamic_pool detail
Interface: mams-4/0/0, Service set: dynamic_nat44_set
NAT pool: dynamic_pool, Translation type: DYNAMIC NAT44
Address range: 16.1.1.0-16.1.1.84
Address range: 16.1.1.255-16.1.1.255
Out of address errors: 0, Addresses in use: 0

```



```
Interface: mams-4/1/0, Service set: dynamic_nat44_set
NAT pool: dynamic_pool, Translation type: DYNAMIC NAT44
Address range: 16.1.1.85-16.1.1.169
Out of address errors: 0, Addresses in use: 0
```

```
Interface: mams-5/0/0, Service set: dynamic_nat44_set
NAT pool: dynamic_pool, Translation type: DYNAMIC NAT44
Address range: 16.1.1.170-16.1.1.254
Out of address errors: 0, Addresses in use: 0
```

show services nat statistics

Syntax `show services nat statistics`
`<interface interface>`

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 interface`—Name of the extension provider interface.

Required Privilege Level view

List of Sample Output [show services nat statistics on page 999](#)

Output Fields [Table 83 on page 994](#) 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 83: 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 83: 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 83: 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 83: 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 83: 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 83: 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
                             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 1003 |
| Output Fields | Table 84 on page 1003 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 84: 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 on page 1007](#)
[show services sessions brief on page 1009](#)
[show services sessions interface mams-5/0/0 extensive on page 1009](#)
[show services sessions terse on page 1010](#)
[show services sessions count on page 1011](#)

Output Fields

[Table 85 on page 1007](#) lists the output fields for the **show services sessions** command. Output fields are listed in the approximate order in which they appear.

Table 85: show services sessions Output Fields

| Field Name | Field Description |
|--------------------------|--|
| Interface | Name of the interface. |
| 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 <i>source-prefix:port</i> . 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
                        mams-4/0/0
                        Session: 12486462, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,

```

```

Asymmetric: no
UDP      10.10.10.2:27    ->    20.20.59.15:10001 Forward I      16018
UDP      20.20.59.15:10001 ->    40.1.31.221:1025 Forward O      0
Session: 12472092, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.2:6     ->    20.20.58.250:10001 Forward I      16006
UDP      20.20.58.250:10001 ->    40.1.31.220:1025 Forward O      0
Session: 587492, ALG: none, Flags: 0x0000, IP Action: no, Offload: no, Asymmetric:
no
UDP      10.10.10.2:18    ->    20.20.59.6:10001 Forward I      16004
UDP      20.20.59.6:10001 ->    40.1.31.218:1025 Forward O      0
Session: 12492907, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.2:15    ->    20.20.59.3:10001 Forward I      16011
UDP      20.20.59.3:10001 ->    40.1.31.219:1025 Forward O      0
Session: 561592, ALG: none, Flags: 0x0000, IP Action: no, Offload: no, Asymmetric:
no
UDP      10.10.10.2:3     ->    20.20.58.247:10001 Forward I      16014
UDP      20.20.58.247:10001 ->    40.1.31.216:1025 Forward O      0
Session: 12449254, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.2:12    ->    20.20.59.0:10001 Forward I      16028
UDP      20.20.59.0:10001 ->    40.1.31.217:1025 Forward O      0
[...output truncated...]
mams-4/1/0
Session: 12243036, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.3:25    ->    20.20.59.13:10001 Forward I      16017
UDP      20.20.59.13:10001 ->    40.1.119.226:1025 Forward O      0
Session: 12243956, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.3:28    ->    20.20.59.16:10001 Forward I      16023
UDP      20.20.59.16:10001 ->    40.1.119.223:1025 Forward O      0
Session: 12199229, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.3:22    ->    20.20.59.10:10001 Forward I      16052
UDP      20.20.59.10:10001 ->    40.1.119.225:1025 Forward O      0
Session: 12197363, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.3:13    ->    20.20.59.1:10001 Forward I      16041
UDP      20.20.59.1:10001 ->    40.1.119.224:1025 Forward O      0
Session: 12486923, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.3:16    ->    20.20.59.4:10001 Forward I      15993
UDP      20.20.59.4:10001 ->    40.1.119.221:1025 Forward O      0
Session: 12212620, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.3:7     ->    20.20.58.251:10001 Forward I      16020
UDP      20.20.58.251:10001 ->    40.1.119.222:1025 Forward O      0
[...output truncated...]
mams-5/0/0
Session: 12453894, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.4:8     ->    20.20.58.252:10001 Forward I      16021
UDP      20.20.58.252:10001 ->    40.1.211.60:1025 Forward O      0
Session: 12485633, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.4:29    ->    20.20.59.17:10001 Forward I      16009
UDP      20.20.59.17:10001 ->    40.1.211.61:1025 Forward O      0
Session: 12434995, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no

```



```

UDP      10.10.10.4:20    ->    20.20.59.8:10001 Forward  I          16023
UDP      20.20.59.8:10001 ->    40.1.211.58:1025 Forward  0              0
Session: 12478616, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.4:17    ->    20.20.59.5:10001 Forward  I          16012
UDP      20.20.59.5:10001 ->    40.1.211.59:1025 Forward  0              0
Session: 12411414, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.4:14    ->    20.20.59.2:10001 Forward  I          15954
UDP      20.20.59.2:10001 ->    40.1.211.57:1025 Forward  0              0
Session: 12348030, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.4:11    ->    20.20.58.255:10001 Forward  I          16002
UDP      20.20.58.255:10001 ->    40.1.211.55:1025 Forward  0              0
[...output truncated...]

```

show services sessions brief The output for the **show services flows brief** command is identical to that for the **show services sessions** command. For sample output, see [show services sessions on page 1007](#).

show services sessions interface mams-5/0/0 extensive

```

user@host> show services sessions interface mams-5/0/0 extensive
mams-5/0/0
Session: 12453894, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
NAT Pugin Data:
  NAT Action: Translation Type - NAPT-44
  NAT source  10.10.10.4:8    ->    40.1.211.60:1025
UDP      10.10.10.4:8    ->    20.20.58.252:10001 Forward  I          20043
  Byte count: 27077166
  Flow role: Initiator, Timeout: 0
UDP      20.20.58.252:10001 ->    40.1.211.60:1025 Forward  0              0
  Byte count: 0
  Flow role: Responder, Timeout: 0
Session: 12485633, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no

NAT Pugin Data:
  NAT Action: Translation Type - NAPT-44
  NAT source  10.10.10.4:29   ->    40.1.211.61:1025
UDP      10.10.10.4:29   ->    20.20.59.17:10001 Forward  I          20031
  Byte count: 27076614
  Flow role: Initiator, Timeout: 0
UDP      20.20.59.17:10001 ->    40.1.211.61:1025 Forward  0              0
  Byte count: 0
  Flow role: Responder, Timeout: 0
Session: 12434995, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no

NAT Pugin Data:
  NAT Action: Translation Type - NAPT-44
  NAT source  10.10.10.4:20   ->    40.1.211.58:1025
UDP      10.10.10.4:20   ->    20.20.59.8:10001 Forward  I          20045
  Byte count: 27077258
  Flow role: Initiator, Timeout: 0
UDP      20.20.59.8:10001 ->    40.1.211.58:1025 Forward  0              0
  Byte count: 0
  Flow role: Responder, Timeout: 0
Session: 12478616, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no

```

[...output truncated...]

```

show services sessions user@router> show services sessions terse
terse mams-4/0/0
Session: 12486462, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.2:27    ->    20.20.59.15:10001 Forward I          23320
UDP      20.20.59.15:10001 ->    40.1.31.221:1025 Forward O          0
Session: 12472092, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.2:6     ->    20.20.58.250:10001 Forward I          23308
UDP      20.20.58.250:10001 ->    40.1.31.220:1025 Forward O          0
Session: 587492, ALG: none, Flags: 0x0000, IP Action: no, Offload: no, Asymmetric:
no
UDP      10.10.10.2:18    ->    20.20.59.6:10001 Forward I          23306
UDP      20.20.59.6:10001 ->    40.1.31.218:1025 Forward O          0
Session: 12492907, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.2:15    ->    20.20.59.3:10001 Forward I          23313
UDP      20.20.59.3:10001 ->    40.1.31.219:1025 Forward O          0
Session: 561592, ALG: none, Flags: 0x0000, IP Action: no, Offload: no, Asymmetric:
no
UDP      10.10.10.2:3     ->    20.20.58.247:10001 Forward I          23316
UDP      20.20.58.247:10001 ->    40.1.31.216:1025 Forward O          0
[...output truncated...]
mams-4/1/0
Session: 12243036, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.3:25    ->    20.20.59.13:10001 Forward I          23319
UDP      20.20.59.13:10001 ->    40.1.119.226:1025 Forward O          0
Session: 12243956, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.3:28    ->    20.20.59.16:10001 Forward I          23325
UDP      20.20.59.16:10001 ->    40.1.119.223:1025 Forward O          0
Session: 12199229, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.3:22    ->    20.20.59.10:10001 Forward I          23354
UDP      20.20.59.10:10001 ->    40.1.119.225:1025 Forward O          0
Session: 12197363, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.3:13    ->    20.20.59.1:10001 Forward I          23343
UDP      20.20.59.1:10001 ->    40.1.119.224:1025 Forward O          0
Session: 12486923, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.3:16    ->    20.20.59.4:10001 Forward I          23295
UDP      20.20.59.4:10001 ->    40.1.119.221:1025 Forward O          0
[...output truncated...]
mams-5/0/0
Session: 12453894, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.4:8     ->    20.20.58.252:10001 Forward I          23323
UDP      20.20.58.252:10001 ->    40.1.211.60:1025 Forward O          0
Session: 12485633, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.4:29    ->    20.20.59.17:10001 Forward I          23311
UDP      20.20.59.17:10001 ->    40.1.211.61:1025 Forward O          0
Session: 12434995, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.4:20    ->    20.20.59.8:10001 Forward I          23325
UDP      20.20.59.8:10001 ->    40.1.211.58:1025 Forward O          0

```

```

Session: 12478616, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.4:17    ->    20.20.59.5:10001 Forward I      23314
UDP      20.20.59.5:10001 ->    40.1.211.59:1025 Forward 0      0
Session: 12411414, ALG: none, Flags: 0x0000, IP Action: no, Offload: no,
Asymmetric: no
UDP      10.10.10.4:14    ->    20.20.59.2:10001 Forward I      23256
UDP      20.20.59.2:10001 ->    40.1.211.57:1025 Forward 0      0
[...output truncated...]

```

```

show services sessions count user@host> show services sessions count
                                Interface  Service set                Sessions count
                                mams-4/0/0  Src_static                  10000
                                mams-4/1/0  Src_static                  10000
                                mams-5/0/0  Src_static                  10000

```


CHAPTER 37

System Architecture Operational Commands

show unified-edge ggsn-pgw call-rate statistics

| | |
|---------------------------------|--|
| Syntax | show unified-edge ggsn-pgw call-rate statistics <history> |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Display the call-rate statistics for the broadband gateway. |
| Options | <p>none—Display the call-rate statistics for the broadband 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.)</p> |
| Required Privilege Level | view |
| List of Sample Output | show unified-edge ggsn-pgw call-rate statistics on page 1015 show unified-edge ggsn-pgw call-rate statistics history on page 1015 |
| Output Fields | Table 86 on page 1014 lists the output fields for the show unified-edge ggsn-pgw call-rate statistics command. Output fields are listed in the approximate order in which they appear. |

Table 86: show unified-edge ggsn-pgw call-rate statistics Output Fields

| Field Name | Field Description |
|-----------------------------------|--|
| Record | Record number for the interval in which the call-rate statistics were 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 information related to the control plane 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. |
| Data Plane (Gn) | <p>The following information related to the data plane (Gn interface) 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 at which the call-rate statistics for the record were computed. |

Sample Output

```

show unified-edge      user@host> show unified-edge ggsn-pgw call-rate statistics
ggsn-pgw call-rate    Record 1 (Call-rate statistics for the past 5 min):
statistics            Control Plane:
                        Activations:    0
                        Deactivations:  0
                        Data Plane(Gn):
                        Input Packets:    0
                        Output packets:  0
                        Input bytes:     0
                        Output bytes:    0
                        Statistics collection time: 2011-05-05 00:25:49 PDT (00:01:06 ago)

show unified-edge      user@host> show unified-edge ggsn-pgw call-rate statistics history
ggsn-pgw call-rate    Record 1 (Call-rate statistics for the past 5 min):
statistics history    Control Plane:
                        Activations:    10
                        Deactivations:  0
                        Data Plane(Gn):
                        Input Packets:    600
                        Output packets:  600
                        Input bytes:     556800
                        Output bytes:    556800
                        Statistics collection time: 2011-05-19 02:33:05 PDT (00:01:19 ago)

                        Record 2 (Call-rate statistics for the past 5 min):
                        Control Plane:
                        Activations:     4294967286
                        Deactivations:    0
                        Data Plane(Gn):
                        Input Packets:    18446744073709550781
                        Output packets:  18446744073709550781
                        Input bytes:     18446744073709474796
                        Output bytes:    18446744073709474796
                        Statistics collection time: 2011-05-19 02:28:05 PDT (00:06:19 ago)

                        Record 3 (Call-rate statistics for the past 5 min):
                        Control Plane:
                        Activations:      9
                        Deactivations:    4294967295
                        Data Plane(Gn):
                        Input Packets:    774
                        Output packets:  774
                        Input bytes:     20212
                        Output bytes:    20212
                        Statistics collection time: 2011-05-19 02:23:05 PDT (00:11:19 ago)

```

show unified-edge ggsn-pgw resource-manager clients

| | |
|---------------------------------|--|
| Syntax | show unified-edge ggsn-pgw resource-manager clients |
| Release Information | Command introduced in Junos OS Mobility Release 11.2W. |
| Description | Display information about the resource management clients (the session Dense Port Concentrators [DPCs] and interface DPCs and Modular Port Concentrators [MPCs]) on the broadband gateway. |
| Options | This command has no options. |
| Required Privilege Level | view |
| List of Sample Output | show unified-edge ggsn-pgw resource-manager clients on page 1016 |
| Output Fields | Table 87 on page 1016 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 87: 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 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 is able to handle session creation requests. |
| Role | Role of the resource manager client slot: <ul style="list-style-type: none"> • Primary—Indicates that the resource manager client is a primary member. • Secondary—Indicates that the resource manager client is a secondary or backup member. |

Sample Output

```

show unified-edge user@host> show unified-edge ggsn-pgw resource-manager clients
ggsn-pgw
resource-manager
clients
Client      State      Redundancy
              Role
pfe-1/2/0   In-Service Primary
pfe-1/0/0   In-Service Primary
pfe-2/2/0   In-Service Primary
pfe-2/0/0   In-Service Primary
pfe-3/2/0   In-Service Primary
pfe-3/0/0   In-Service Primary
pfe-4/2/0   In-Service Primary
pfe-4/0/0   In-Service Primary
ms-7/0/0     In-Service Secondary
ms-7/1/0     In-Service Secondary
ms-8/0/0     In-Service Primary
ms-8/1/0     In-Service Primary
ms-9/0/0     In-Service Primary

```



```
ms-9/1/0 In-Service Primary  
ms-10/0/0 In-Service Secondary  
ms-10/1/0 In-Service Secondary
```


PART 13

Index

- [Index on page 1021](#)
- [Index of Statements and Commands on page 1039](#)

Index

Symbols

| | |
|--|--------|
| #, comments in configuration statements..... | xxxiv |
| (), in syntax descriptions..... | xxxiv |
| 3G networks | |
| broadband gateway..... | 22 |
| GGSN..... | 31 |
| < >, in syntax descriptions..... | xxxiii |
| [], in configuration statements..... | xxxiv |
| { }, in configuration statements..... | xxxiv |
| (pipe), in syntax descriptions..... | xxxiv |

A

| | |
|--|----------|
| AAA | |
| AAA profile configuration example..... | 160 |
| configuration example..... | 152 |
| configuration overview..... | 108 |
| configuration steps..... | 139 |
| configuring RADIUS servers..... | 139 |
| network element group configuration | |
| example..... | 160 |
| network elements..... | 111 |
| network elements configuration example..... | 159 |
| RADIUS configuration example..... | 155 |
| scalability and redundancy features..... | 110 |
| server failover..... | 111 |
| verifying the configuration..... | 163 |
| AAA profile..... | 109 |
| accounting options..... | 145 |
| applying to an APN..... | 150 |
| authentication options..... | 144 |
| configuration example..... | 160 |
| configuration steps..... | 144 |
| excluding or ignoring RADIUS attributes..... | 146 |
| overview..... | 113 |
| RADIUS options..... | 114, 150 |
| aaa statement..... | 470 |
| APN..... | 553 |
| AAA troubleshooting..... | 387 |
| aaa-override statement | |
| APN..... | 554 |

| | |
|---|----------|
| aaa-profile statement | |
| APN..... | 555 |
| aaa-radius statement..... | 488 |
| access point name..... | 336 |
| access point name delete | 336 |
| access point name modify..... | 322 |
| Access-Accept messages..... | 119 |
| Access-Request messages..... | 115 |
| accounting | |
| AAA profile options..... | 113, 145 |
| network element groups..... | 112, 143 |
| overview..... | 109 |
| Accounting On messages..... | 135 |
| Accounting Start messages..... | 122 |
| accounting statement | |
| unified-edge profile..... | 472 |
| Accounting Stop messages..... | 131 |
| accounting-port statement..... | 473 |
| accounting-secret statement..... | 473 |
| activate maintenance mode..... | 323 |
| address assignment | |
| APN configuration..... | 89 |
| by the AAA server..... | 151, 152 |
| configuring AAA server override..... | 151 |
| address statement..... | 474 |
| address-assignment statement | |
| APN..... | 556 |
| MobileNext Broadband Gateway..... | 502 |
| ageing-window statement | |
| mobile pools..... | 503 |
| aggregate maximum bit rate See AMBR | |
| aggregated-maximum-bit-rate statement | |
| cos-cac..... | 693 |
| algorithm statement..... | 474 |
| allocation and retention priority See ARP | |
| allocation and retention-priority statement | |
| cos-cac..... | 694 |
| allow-dynamic-requests statement..... | 475 |
| allow-static-ip-address statement | |
| APN..... | 557 |
| AMBR | |
| configuring | |
| downlink..... | 266, 270 |
| uplink..... | 266, 270 |
| overview..... | 244, 247 |
| anchor interface DPCs and MPCs | |
| exceptions..... | 64 |
| anchor session DPCs | |
| exceptions..... | 64 |

| | |
|--|-------------|
| anchor-pfes statement..... | 529 |
| anchor-spics statement..... | 530 |
| anchoring-options statement..... | 531 |
| anchors | |
| broadband gateway..... | 45, 56 |
| configuring on broadband gateway..... | 47 |
| anonymous users | |
| APN configuration..... | 88 |
| anonymous-user statement | |
| APN..... | 558 |
| apfe-group-set statement..... | 532 |
| APN | |
| configuration example..... | 100 |
| apn-data-type statement | |
| APN..... | 559 |
| apn-name statement | |
| service selection profiles..... | 604 |
| apn-services statement..... | 560 |
| apn-type statement | |
| APN..... | 562 |
| APNs | |
| AAA configuration example..... | 162 |
| applying an AAA profile..... | 150 |
| broadband gateway..... | 79, 94, 96 |
| configuring address assignment..... | 87, 89, 151 |
| configuring anonymous users..... | 88 |
| configuring charging profiles..... | 93 |
| configuring general APN parameters..... | 83 |
| configuring QoS local policy profiles..... | 93 |
| configuring service selection..... | 97 |
| mobile network..... | 28 |
| apns statement..... | 563 |
| APN services..... | 563 |
| architecture | |
| 3G networks..... | 22 |
| ARP..... | 244 |
| in 3G networks..... | 244 |
| in 4G networks..... | 244 |
| overview..... | 244 |
| See also preemption | |
| attributes statement..... | 476 |
| AuC | |
| mobile network..... | 32 |
| authentication | |
| AAA profile options..... | 113, 144 |
| overview..... | 108 |
| authentication statement..... | 477 |
| authentication-port statement..... | 477 |

B

| | |
|--|----------|
| background traffic class | |
| configuring..... | 264 |
| description..... | 241 |
| bandwidth pools..... | 245 |
| allocating for conversational traffic class..... | 255 |
| allocating for streaming traffic class..... | 255 |
| configuring..... | 255 |
| APN level..... | 245 |
| downlink..... | 273 |
| system level..... | 245, 273 |
| uplink..... | 274 |
| See also overview | |
| bandwidth-pool statement | |
| cos-cac..... | 695 |
| bearer load | |
| configuring | |
| in 3G networks..... | 259 |
| in 3G/4G networks..... | 260 |
| in 4G networks..... | 257 |
| bearer-load statement | |
| cos-cac..... | 696 |
| bearers | |
| configuring maximum number | |
| APN level..... | 254 |
| system level..... | 254 |
| initial QoS level..... | 240 |
| managing load..... | 246 |
| maximum number, at system or APN | |
| level..... | 246 |
| mobile network..... | 30 |
| preempting..... | 246 |
| rejecting based on | |
| AMBR..... | 267, 271 |
| maximum traffic class..... | 247 |
| upgrading based on | |
| AMBR..... | 267, 271 |
| ARP..... | 267 |
| QCI..... | 266 |
| bind-interface statement | |
| dhcp..... | 513 |
| block-visitors statement | |
| APN..... | 565 |
| braces, in configuration statements..... | xxxiv |
| brackets | |
| angle, in syntax descriptions..... | xxxiii |
| square, in configuration statements..... | xxxiv |

| | |
|---|----------|
| broadband gateway | |
| 3G networks..... | 22 |
| address assignment configuration..... | 89 |
| anchors..... | 45, 56 |
| and GGSN..... | 9 |
| and IPv6 protocol..... | 68 |
| anonymous user configuration..... | 88 |
| APN charging profiles configuration..... | 93 |
| APN configuration..... | 79, 83 |
| APN configuration example..... | 100 |
| APN QoS local policy profiles | |
| configuration..... | 93 |
| APN service selection configuration..... | 97 |
| APNs configuration..... | 94, 96 |
| chassis configuration..... | 38 |
| chassis configuration example..... | 43 |
| configuring anchors | 47 |
| configuring call rate statistics..... | 13 |
| configuring fragment reassembly..... | 66 |
| configuring gateways..... | 10 |
| configuring HPLMNs..... | 10 |
| configuring local policies..... | 11 |
| control packet flow..... | 5 |
| downlink payload packet flow..... | 8 |
| exceptions..... | 64, 65 |
| exceptions configuration example..... | 72 |
| general gateway..... | 14 |
| interface DPC or MPC configuration..... | 42 |
| interface redundancy..... | 52 |
| interfaces configuration example..... | 43 |
| interfaces redundancy configuration | |
| example..... | 58 |
| IP fragments..... | 66 |
| IPv6 protocol..... | 67 |
| mobile interface configuration..... | 94, 96 |
| mobile options..... | 16 |
| P-GW..... | 9 |
| physical interface overview..... | 39 |
| QoS configuration example..... | 277 |
| redundancy configuration..... | 50 |
| redundancy configuration example..... | 58 |
| restriction value configuration..... | 87 |
| Routing Engine redundancy..... | 50 |
| session DPC configuration..... | 40 |
| session DPC configuration example..... | 43 |
| session DPC overview..... | 39 |
| session DPC redundancy..... | 51 |
| session DPC redundancy configuration | |
| example..... | 58 |
| system architecture..... | 3 |
| traceoptions..... | 70 |
| uplink payload packet flow..... | 7 |
| user-session routing..... | 81 |
| VRF configuration..... | 96 |
| Broadband Gateway | |
| AAA configuration..... | 108 |
| configuring | |
| QoS, overview..... | 253 |
| GGSN..... | 31 |
| resource manager..... | 18 |
| C | |
| CAC | |
| bandwidth pools..... | 245 |
| enforcing..... | 245 |
| maximum bearers..... | 246 |
| overview..... | 245 |
| preemption, enabling..... | 256 |
| resource thresholds..... | 246 |
| call admission control See CAC | |
| call admission control troubleshooting..... | 385 |
| call detail record profile change..... | 331 |
| call rate statistics | |
| configuring on broadband gateway..... | 13 |
| monitoring..... | 13 |
| call-rate-statistics statement..... | 779 |
| CDR profiles | |
| configuring..... | 229 |
| cdr-aggregation-limit statement..... | 619 |
| cdr-profile statement..... | 620 |
| cdr-profiles statement..... | 621 |
| cdr-release statement | |
| charging-gateways..... | 622 |
| CDRs | |
| GTP Prime properties..... | 220 |
| cds-per-file statement..... | 623 |
| Change of Authorization (CoA) Messages..... | 137 |
| charging | |
| configuring..... | 219 |
| disabling persistent storage..... | 882 |
| enabling persistent storage..... | 881 |
| charging configurations | |
| managing..... | 235 |
| monitoring..... | 235 |
| charging gateway statistics..... | 358 |
| charging profile change..... | 326, 337 |
| charging profile delete..... | 330 |

| | | |
|---|--------|--|
| charging profiles | | |
| APN | | |
| configuring..... | 232 | |
| APN configuration..... | 93 | |
| CDR profiles..... | 229 | |
| configuring..... | 231 | |
| transport profiles..... | 226 | |
| trigger profiles..... | 227 | |
| charging statement..... | 624 | |
| APN..... | 566 | |
| charging-characteristics statement | | |
| service selection profiles..... | 605 | |
| charging-gateways statement..... | 627 | |
| charging-profiles statement..... | 628 | |
| chassis | | |
| broadband gateway..... | 38 | |
| configuration example..... | 43 | |
| monitoring..... | 48 | |
| redundancy configuration..... | 52, 54 | |
| chassis configuration example | | |
| broadband gateway..... | 43 | |
| class-of-service statement..... | 699 | |
| classifier profiles | | |
| configuring | | |
| 3G networks..... | 263 | |
| 4G networks..... | 262 | |
| for 3G and 4G networks..... | 264 | |
| classifier-profile statement | | |
| local-policies..... | 697 | |
| classifier-profiles statement | | |
| cos-cac..... | 698 | |
| clear unified edge ggsn pgw gtp peer statistics | | |
| command..... | 979 | |
| clear unified edge ggsn pgw gtp statistics | | |
| command..... | 978 | |
| clear unified-edge ggsn-pgw aaa radius statistics | | |
| command..... | 810 | |
| clear unified-edge ggsn-pgw aaa statistics | | |
| command..... | 811 | |
| clear unified-edge ggsn-pgw address-assignment | | |
| pool name..... | 812 | |
| clear unified-edge ggsn-pgw address-assignment | | |
| statistics command..... | 813 | |
| clear unified-edge ggsn-pgw charging cdr | | |
| command..... | 876 | |
| clear unified-edge ggsn-pgw charging cdr wfa | | |
| command..... | 877 | |
| clear unified-edge ggsn-pgw charging | | |
| local-persistent-storage statistics | | |
| command..... | 878 | |
| clear unified-edge ggsn-pgw charging path | | |
| statistics command..... | 879 | |
| clear unified-edge ggsn-pgw charging transfer | | |
| statistics command..... | 880 | |
| clear unified-edge ggsn-pgw exception-handling | | |
| statistics command..... | 964 | |
| clear unified-edge ggsn-pgw ip-reassembly | | |
| statistics command..... | 965 | |
| clear unified-edge ggsn-pgw statistics | | |
| command..... | 846 | |
| clear unified-edge ggsn-pgw subscribers charging | | |
| command..... | 849 | |
| clear unified-edge ggsn-pgw subscribers | | |
| command..... | 847 | |
| clear unified-edge ggsn-pgw subscribers peer | | |
| command..... | 850 | |
| client statement | | |
| resource management..... | 792 | |
| comments, in configuration statements..... | xxxiv | |
| configuration | | |
| broadband gateway..... | 38 | |
| broadband gateway interface PFEs..... | 50 | |
| broadband gateway services PICs..... | 50 | |
| configuration example | | |
| APN..... | 100 | |
| chassis..... | 43 | |
| exceptions..... | 72 | |
| for QoS..... | 277 | |
| redundancy..... | 58 | |
| configuring address assignment | | |
| APN configuration..... | 89 | |
| configuring anonymous users | | |
| APN configuration..... | 88 | |
| configuring APNs | | |
| gateways configuration..... | 10 | |
| configuring broadband gateway | | |
| APN configuration..... | 79, 83 | |
| configuring call rate statistics | | |
| gateways configuration..... | 13 | |
| configuring charging profiles | | |
| APNs..... | 93 | |
| configuring chassis | | |
| interfaces for mobility redundancy..... | 54 | |
| session DPC redundancy..... | 52 | |
| configuring HPLMNs | | |
| gateways..... | 10 | |

| | |
|--|--------|
| configuring interface DPCs or MPCs | |
| user traffic..... | 42 |
| configuring interfaces for mobility | |
| redundancy..... | 54 |
| configuring local policies | |
| gateways..... | 11 |
| configuring mobile interfaces | |
| mobility..... | 94, 96 |
| configuring PFEs | |
| anchor configuration..... | 47 |
| configuring QoS local policy profiles | |
| APNs..... | 93 |
| configuring redundancy | |
| interfaces for mobility..... | 54 |
| session DPC..... | 52 |
| configuring restriction value | |
| APN configuration..... | 87 |
| configuring service selection | |
| APNs..... | 97 |
| configuring session DPC | |
| control messages..... | 40 |
| redundancy..... | 52 |
| configuring session DPCs | |
| anchor configuration..... | 47 |
| connection set identifiers..... | 184 |
| container-limit statement..... | 629 |
| control messages | |
| session DPC configuration..... | 40 |
| control packet flow | |
| broadband gateway..... | 5 |
| control plane | |
| configuring GTP services | |
| for GGSN/P-GW..... | 190 |
| control statement | |
| gtp statement..... | 751 |
| conventions | |
| text and syntax..... | xxxiii |
| conversational traffic class | |
| configuring..... | 263 |
| description..... | 241 |
| CoS policy profile | |
| AMBR in..... | 247 |
| configuring | |
| in 3G networks..... | 268 |
| in 3G/4G networks..... | 270 |
| in 4G networks..... | 266 |
| GBR in..... | 248 |
| maximum QCI in..... | 247 |
| maximum traffic class in..... | 247 |
| MBR in..... | 247 |
| overview..... | 247 |
| policer actions..... | 248 |
| cos-cac statement..... | 700 |
| cos-policy-profile statement | |
| local-policies..... | 702 |
| cos-policy-profiles statement | |
| cos-cac..... | 703 |
| CPU | |
| managing load | 246 |
| CPU load | |
| configuring | |
| in 3G networks..... | 259 |
| in 3G/4G networks..... | 261 |
| in 4G networks..... | 257 |
| cpu statement | |
| cos-cac..... | 704 |
| curly braces, in configuration statements..... | xxxiv |
| current-hop-limit statement | |
| IPv6 router advertisement..... | 731 |
| customer support..... | xxxiv |
| contacting JTAC..... | xxxiv |
| D | |
| data plane | |
| configuring GTP services | |
| for GGSN/P-GW..... | 192 |
| data rate statistics..... | 359 |
| data statement | |
| gtp statement..... | 752 |
| dead server detection..... | 112 |
| configuring..... | 141 |
| dead-criteria-retries statement..... | 478 |
| dead-server-retry-interval statement | |
| dhcp..... | 514 |
| dead-server-successive-retry-attempt statement | |
| dhcp..... | 515 |
| default settings | |
| preemption..... | 253 |
| resource thresholds | 247 |
| default-pool statement | |
| mobile pools..... | 503 |
| default-profile statement | |
| APN..... | 567 |
| default-rating-group statement..... | 629 |
| default-service-id statement..... | 630 |
| delete access point name..... | 325 |
| deployment | |
| mobile network..... | 32 |

| | | | |
|---|-------|--|-----|
| description statement | | DSCP marking | |
| APN..... | 568 | subscriber packets..... | 276 |
| cdr-profiles..... | 631 | dscp-code-point statement | |
| charging-profiles..... | 631 | gtp statement..... | 752 |
| transport-profiles..... | 631 | dscp-ipv6-rewrite-rule-name statement | |
| trigger-profiles..... | 631 | class-of-service..... | 705 |
| destination-ipv4-address statement..... | 632 | dscp-ipv6-rewrite-rule-name-ingress statement | |
| destination-port statement | | class-of-service..... | 706 |
| gtp..... | 633 | dscp-rewrite-rule-name statement | |
| DHCP | | class-of-service..... | 706 |
| AAA address override..... | 151 | dscp-rewrite-rule-name-ingress statement | |
| configuring..... | 168 | class-of-service..... | 707 |
| APN..... | 169 | dynamic requests..... | 110 |
| dhcp-proxy-client statement | | enabling for a RADIUS server..... | 141 |
| APN..... | 569 | dynamic-requests-secret statement..... | 478 |
| dhcp..... | 516 | E | |
| dhcp-server-selection-algorithm statement | | echo interval | |
| dhcp..... | 517 | gtp..... | 753 |
| dhcpcv4-profiles statement | | echo-interval statement | |
| dhcp..... | 518 | gtp..... | 638 |
| dhcpcv4-proxy-client-profile statement | | echo-n3-requests statement | |
| APN..... | 570 | gtp statement..... | 753 |
| dhcpcv6-profiles statement | | echo-t3-response statement | |
| dhcp..... | 519 | gtp statement..... | 754 |
| dhcpcv6-proxy-client-profile statement | | edit access address-assignment statement | |
| APN..... | 571 | hierarchy..... | 448 |
| diffserv model | | edit interfaces ams statement hierarchy..... | 449 |
| QoS support on broadband gateway..... | 240 | edit interfaces apfe statement hierarchy..... | 450 |
| direction statement..... | 634 | edit interfaces mif statement hierarchy..... | 450 |
| disable statement | | edit services ip-reassembly statement | |
| IPv6 router advertisement..... | 732 | hierarchy..... | 452 |
| disable-replication statement..... | 635 | edit services service-set statement hierarchy..... | 452 |
| Disconnect Request messages..... | 136 | edit unified-edge mobile-options statement | |
| disk-space-policy statement..... | 636 | hierarchy..... | 466 |
| dl-bandwidth-pool statement | | edit unified-edge resource-management statement | |
| local-policies..... | 705 | hierarchy..... | 466 |
| dns-server statement | | egress rewrite rules | |
| APN..... | 572 | configuring..... | 275 |
| documentation | | overview | |
| comments on..... | xxxiv | overview..... | 249 |
| down-detect-time statement | | egress-key statement | |
| gtp..... | 637 | aggregated multiservices..... | 771 |
| downlink payload packet flow | | EIR | |
| broadband gateway..... | 8 | mobile network..... | 32 |
| DPCs | | enable-reduced-partial-cdrs statement..... | 639 |
| configuring interface DPCs..... | 42 | enable-rejoin statement | |
| drop-member-traffic statement | | aggregated multiservices..... | 534 |
| aggregated multiservices..... | 533 | | |

-
- EPC
 - mobile network.....26
 - error-indication-interval statement.....732
 - gtp statement.....754
 - errors
 - exceptions.....65
 - evolved packet core
 - mobile network.....26
 - exceed-action policer
 - configuring
 - for GBR.....269
 - overview.....248
 - exceed-action statement
 - cos-cac.....707
 - exceptions
 - broadband gateway.....64, 65
 - configuration example.....72
 - traceoptions.....70
 - exclude statement.....479
 - trigger-profiles.....640
 - exclude-ie-options statement.....642
 - exclude-pools statement
 - APN.....573
 - exclude-v6pools statement
 - APN.....574
 - exit maintenance mode.....324
 - external-assigned statement
 - mobile pools.....504
- F**
- failover
 - broadband gateway anchors.....56
 - family statement
 - aggregated multiservices.....535
 - mobile interface.....780
 - mobile pools.....505
 - file-age statement.....646
 - file-creation-policy statement.....647
 - file-format statement.....648
 - file-name-private-extension statement.....649
 - file-size statement.....650
 - filter statement
 - mobile interface.....780
 - font conventions.....xxxiii
 - forwarding classes
 - mapping to QCI values.....262
 - mapping to traffic classes.....263
 - forwarding-class statement
 - gtp statement.....755
 - forwarding-packages statement.....781
 - fragment
 - broadband gateway handling.....66
 - fragment reassembly
 - configuring on broadband gateway.....66
 - from statement
 - service selection profiles.....606
 - functions in mobile network
 - APNs.....28
 - packet data network gateway.....25
- G**
- gateway configurations
 - monitoring.....13
 - gateways
 - configuring on broadband gateway.....10
 - GBR
 - configuring in traffic classes.....269
 - overview.....242, 248
 - GBR bearers.....245
 - See also* bandwidth pools
 - general gateway
 - traceoptions.....14
 - GGSN
 - broadband gateway.....9, 31
 - functions in mobile network.....21, 24
 - in 3G networks.....31
 - ggsn-pgw statement.....782
 - Gi to Gn data packets trace.....370
 - Gn interface
 - configuring GTP services
 - for GGSN/P-GW.....196
 - gn statement
 - gtp statement.....756
 - Gn to Gi (GTP-U) data packet trace366
 - Gp interface
 - configuring GTP services
 - for GGSN/P-GW.....198
 - gp statement
 - gtp statement.....757
 - GPRS Tunneling Protocol.....320
 - group statement
 - APN.....575
 - GTP
 - connection set identifiers.....184
 - echo requests
 - version support for.....177
 - GPRS interfaces.....175
 - overview.....175

| | | | |
|--|----------|---|-------|
| path management | 176 | GTP-C messages | |
| default settings..... | 176 | route lookup..... | 185 |
| disabling..... | 206 | GTP-U errors | |
| echo requests..... | 177 | exceptions..... | 65 |
| echo-request messages..... | 177 | gtp statement..... | 651 |
| overview..... | 176 | guaranteed bit rate <i>See</i> GBR | |
| path failure..... | 178 | guaranteed-bit-rate statement | |
| path success..... | 177 | cos-cac..... | 708 |
| restart counters..... | 183 | H | |
| supported versions..... | 174 | hash-keys statement | |
| tunnel endpoint identifiers..... | 185 | aggregated multiservices..... | 772 |
| tunnel management | | header-type statement | |
| create requests..... | 181 | gtp..... | 652 |
| default settings..... | 180 | high statement | |
| overview..... | 180 | cos-cac..... | 709 |
| path failure..... | 182 | high-availability-options statement | |
| path success..... | 181 | aggregated multiservices..... | 536 |
| request messages..... | 181 | history statement | |
| update/delete requests..... | 181, 182 | call-rate statistics..... | 782 |
| version support..... | 180 | home users | |
| tunnel management functions..... | 180 | mobile network..... | 10 |
| GTP interface address change..... | 319 | home-plmn statement..... | 783 |
| GTP interface delete..... | 320 | home-profile statement | |
| GTP Prime peers | | APN..... | 576 |
| GTP Prime properties..... | 221 | HSS | |
| GTP Prime properties | | mobile network..... | 32 |
| configuring..... | 220, 221 | I | |
| GTP redirect <i>See</i> user-session routing | | icons defined, notice..... | xxxii |
| GTP services | | idle-timeout statement | |
| configuring | | APN..... | 577 |
| 3GPP interfaces in different VRFs..... | 202 | idle-timeout-direction statement | |
| control plane for GGSN/P-GW..... | 190 | APN..... | 578 |
| data plane for GGSN/P-GW..... | 192 | ignore statement..... | 481 |
| default settings..... | 187 | imei statement | |
| GGSN..... | 204 | service selection profiles..... | 607 |
| GGSN/P-GW..... | 189 | imsi statement | |
| Gn interface..... | 196 | service selection profiles..... | 608 |
| Gp interface..... | 198 | inet-pool statement | |
| loopback address..... | 188 | APN..... | 579 |
| peer group..... | 205 | inet-precedence-rewrite-rule-name statement | |
| S5 and S8 interfaces..... | 199, 201 | class-of-service..... | 709 |
| S5 interface..... | 193 | inet-precedence-rewrite-rule-name-ingress | |
| S8 interface..... | 195 | statement | |
| trace options..... | 207 | class-of-service..... | 710 |
| configuring on gateway | | inet6-pool statement | |
| overview..... | 186 | APN..... | 580 |
| GTP signaling..... | 354, 382 | | |
| gtp statement | | | |
| gtp statement..... | 758 | | |

| | |
|---|----------|
| information element (IE) | |
| initial QoS level..... | 240 |
| ingress rewrite rules | |
| configuring..... | 274 |
| overview | |
| overview..... | 249 |
| ingress-key statement | |
| aggregated multiservices..... | 773 |
| ingress-rewrite-rules statement | |
| class of service..... | 710 |
| input statement | |
| mobile interface..... | 783 |
| inter-mobile-traffic statement | |
| APN..... | 581 |
| interactive traffic class | |
| configuring..... | 264 |
| description..... | 241 |
| interface configuration example | |
| broadband gateway..... | 43 |
| interface DPC and MPC | |
| anchors..... | 45 |
| interface DPCs or MPCs | |
| configuring for user traffic..... | 42 |
| interface mobile interfaces | |
| configuring..... | 94, 96 |
| interface redundancy configuration example | |
| broadband gateway..... | 58 |
| interface statement..... | 784 |
| anchor Packet Forwarding Engine..... | 537 |
| gtp statement..... | 761 |
| multiservices PIC..... | 538 |
| interface-service statement | |
| aggregated multiservices..... | 774 |
| interfaces | |
| mobile | |
| applying rewrite rules..... | 276 |
| interfaces for mobility | |
| redundancy configuration..... | 54 |
| interfaces statement | |
| aggregated multiservices..... | 539 |
| aggregated Packet Forwarding Engine..... | 540 |
| class-of-service..... | 711 |
| mobile interface..... | 785 |
| Interim-Update messages..... | 126 |
| interval statement | |
| call-rate statistics..... | 786 |
| IP fragments | |
| broadband gateway handling..... | 66 |
| ip-reassembly statement..... | 733 |
| ip-reassembly-profile statement..... | 734 |
| IPv6 | |
| mobile network..... | 34 |
| IPv6 protocols | |
| broadband gateway parameters..... | 67, 68 |
| ipv6-router-advertisement statement..... | 735 |
| J | |
| jnxMbgPgWGtpPeerDNThresPerPeerNotif | |
| trap..... | 384 |
| jnxMbgPgWGtpPeerDownNotif trap..... | 383 |
| jnxMbgPgWGtpPeerGWUpNotif trap..... | 383 |
| jnxMbgPgWSMBearersThresGblNotif trap..... | 385 |
| jnxMbgPgWSMBearersThresPerSPNotif trap..... | 385 |
| jnxMbgPgWSMGtpEventNotif trap..... | 384 |
| jnxMbgPgWSMSessionEstFailThresPerTCNotf | |
| trap..... | 385 |
| jnxMbgPgWSMSubscribersThresGblNotif | |
| trap..... | 384 |
| jnxMbgPgWSMSubscribersThresPerSPNotif | |
| trap..... | 384, 385 |
| L | |
| lease-time statement | |
| dhcp..... | 520 |
| load-balancing-options statement | |
| aggregated multiservices..... | 541, 775 |
| local policies | |
| configuring on broadband gateway..... | 11 |
| specifying | |
| bandwidth pools..... | 273 |
| classifier profiles..... | 273 |
| policy profiles..... | 273 |
| resource thresholds..... | 273 |
| local policies profile | |
| configuring..... | 273 |
| local policy | |
| applying | |
| system level..... | 274 |
| local statement | |
| APN..... | 582 |
| local-persistent-storage-options statement..... | 653 |
| local-policies..... | 712 |
| local-policy-profile statement | |
| APN..... | 583 |
| MobileNext Broadband Gateway..... | 713 |
| local-storage statement..... | 654 |
| logical-system statement | |
| APN..... | 584 |

| | |
|--|------------|
| loopback address | |
| configuring for GTP services..... | 188 |
| low statement | |
| cos-cac..... | 714 |
| LTE See networks | |
| M | |
| maintenance mode..... | 318 |
| manuals | |
| comments on..... | xxxiv |
| many-to-one statement | |
| aggregated multiservices..... | 542 |
| max-reassembly-pending-packets statement | |
| IP reassembly..... | 736 |
| maximum bearers | |
| configuring | |
| APN level..... | 254 |
| system level..... | 254 |
| maximum bit rate See MBR | |
| maximum pending requests..... | 112 |
| maximum QCI | |
| overview..... | 247 |
| maximum traffic class | |
| overview..... | 247 |
| maximum-advertisement-interval statement | |
| IPv6 router advertisement..... | 737 |
| maximum-bearers statement | |
| APN..... | 585 |
| MobileNext Broadband Gateway..... | 715 |
| service selection profiles..... | 609 |
| maximum-bit-rate statement | |
| cos-cac..... | 716 |
| maximum-initial-advertisement-interval statement | |
| IPv6 router advertisement..... | 738 |
| maximum-initial-advertisements statement | |
| IPv6 router advertisement..... | 739 |
| maximum-pending-reqs-limit statement..... | 481 |
| MBR | |
| configuring in traffic classes..... | 268, 273 |
| overview..... | 242, 247 |
| mcc statement..... | 787 |
| member-failure-options statement | |
| aggregated multiservices..... | 543 |
| member-interface statement | |
| aggregated multiservices..... | 545 |
| memory | |
| managing load | 246 |
| memory load | |
| configuring | |
| in 3G networks..... | 260 |
| in 3G/4G networks..... | 261 |
| in 4G networks..... | 258 |
| Memory monitoring..... | 357 |
| memory statement | |
| cos-cac..... | 717 |
| mif statement | |
| class of service..... | 718 |
| minimum-advertisement-interval statement | |
| IPv6 router advertisement..... | 740 |
| mnc statement..... | 788 |
| mobile address pool change..... | 332 |
| mobile address pool delete..... | 334 |
| mobile charging | |
| flags for tracing operations..... | 234 |
| log filenames for tracing operations..... | 233 |
| tracing operations..... | 233 |
| mobile interface | |
| applying rewrite rules..... | 249 |
| mobile interface change..... | 348 |
| mobile interfaces | |
| applying egress rewrite rules..... | 276 |
| applying ingress rewrite rules..... | 276 |
| configuring | 94, 96 |
| mobile network | |
| 3G..... | 21 |
| 4G/LTE..... | 21 |
| APNs..... | 28 |
| bearers..... | 30 |
| broadband gateway architecture..... | 3 |
| deployment..... | 32 |
| EPC..... | 26 |
| GGSN..... | 21, 24 |
| IPv6..... | 34 |
| P-GW..... | 21, 24, 34 |
| packet data network gateway..... | 25 |
| user types..... | 10 |
| mobile options | |
| traceoptions..... | 16 |
| mobile options statement..... | 793 |
| mobile subscribers | |
| CDR profiles..... | 229 |
| charging profiles..... | 231 |
| APN..... | 232 |
| monitoring..... | 235 |
| persistent storage of CDR..... | 222 |
| tracing operations..... | 233 |

| | |
|---------------------------------------|----------|
| transport profiles..... | 226 |
| trigger profiles..... | 227 |
| mobile-interface statement | |
| APN..... | 586 |
| mobile-pool-groups statement..... | 506 |
| mobile-pools statement..... | 507 |
| mobile-profiles statement..... | 482 |
| mobility address pool delete..... | 346 |
| mobility pool change..... | 340 |
| mobility statement..... | 789 |
| monitoring | |
| chassis configuration..... | 48 |
| MPCs | |
| configuring interface MPCs..... | 42 |
| msisdn statement | |
| service selection profiles..... | 610 |
| mtu statement..... | 655 |
| mobile interface..... | 790 |
| N | |
| n3-requests statement | |
| gtp statement..... | 762 |
| gtp..... | 656 |
| nbns-server statement | |
| APN..... | 587 |
| network element..... | 110 |
| network element group | |
| configuration example..... | 160 |
| specifying for accounting..... | 145 |
| network element groups | |
| configuring..... | 143 |
| overview..... | 112 |
| network elements | |
| configuration example..... | 159 |
| configuring..... | 142 |
| dead server detection..... | 112, 141 |
| load-balancing algorithm..... | 111 |
| maximum pending requests..... | 112 |
| overview..... | 111 |
| server priority..... | 112 |
| specifying for accounting..... | 145 |
| specifying for authentication..... | 144 |
| network statement | |
| mobile pools..... | 508 |
| network-element statement..... | 484 |
| network-element-group statement..... | 484 |
| network-element-groups statement..... | 485 |
| network-elements statement..... | 486 |

| | |
|-------------------------------------|------|
| networks | |
| 3G | |
| ARP..... | 241 |
| classifying subscriber traffic..... | 241 |
| GBR..... | 241 |
| MBR..... | 241 |
| QoS parameters..... | 241 |
| 4G | |
| AMBR..... | 242 |
| ARP..... | 242 |
| classifying subscriber traffic..... | 242 |
| QoS parameters..... | 242 |
| no-address-verify statement | |
| APN..... | 588 |
| no-path-management statement | |
| gtp..... | 657 |
| notice icons defined..... | xxii |
| O | |
| offline charging | |
| configuring..... | 219 |
| offline statement | |
| transport-profiles..... | 658 |
| trigger-profiles..... | 659 |
| options statement | |
| RADIUS..... | 487 |
| output statement | |
| mobile interface..... | 790 |
| overload conditions..... | 381 |
| overview | |
| interface redundancy..... | 52 |
| physical interface types..... | 39 |
| Routing Engine redundancy..... | 50 |
| session DPC..... | 39 |
| session DPC redundancy..... | 51 |
| P | |
| p-cscf statement | |
| APN..... | 589 |
| P-GW | |
| broadband gateway..... | 9 |
| function in mobile network..... | 24 |
| functions in mobile network..... | 21 |
| packet data network gateway | |
| functions in mobile network..... | 25 |
| packet flow | |
| broadband gateway control..... | 5 |
| packet flow downlink | |
| broadband gateway payload..... | 8 |

| | |
|--|----------|
| packet flow uplink | |
| broadband gateway payload..... | 7 |
| packet loss priority See PLP | |
| parentheses, in syntax descriptions..... | xxxiv |
| path management See GTP | |
| path-management statement | |
| gtp statement..... | 763 |
| payload flow downlink | |
| broadband gateway downlink..... | 8 |
| payload flow uplink | |
| broadband gateway uplink..... | 7 |
| PCI flags..... | 244 |
| PCRF | |
| mobile network..... | 32 |
| pdn-type statement | |
| service selection profiles..... | 611 |
| PDP contexts | |
| bearers..... | 30 |
| GBR..... | 242 |
| initial QoS level..... | 240 |
| MBR..... | 242 |
| upgrading based on | |
| ARP..... | 268 |
| highest traffic class..... | 268 |
| MBR..... | 268 |
| peer group | |
| configuring GTP services..... | 205 |
| peer statement | |
| gtp statement..... | 763 |
| gtp..... | 660 |
| peer-order..... | 661 |
| service selection profiles..... | 611 |
| peer-group statement | |
| gtp statement..... | 764 |
| peer-history statement | |
| gtp statement..... | 765 |
| peer-order statement..... | 662 |
| peer-routing-instance statement | |
| service selection profiles..... | 612 |
| pending-queue-size statement | |
| gtp..... | 663 |
| persistent storage | |
| configuring..... | 222 |
| configuring the SSD..... | 224, 225 |
| disabling for charging..... | 882 |
| ejecting the SSD..... | 225 |
| enabling for charging..... | 881 |
| formatting SSD..... | 884 |
| initializing the SSD..... | 225 |
| preparing SSD..... | 883, 884 |
| removing SSD..... | 883 |
| tracing operations..... | 223 |
| persistent-storage-order statement..... | 664 |
| PFE charging statistics..... | 377 |
| physical interfaces | |
| broadband gateway..... | 39 |
| PLMN | |
| mobile network..... | 32 |
| PLMNs | |
| configuring on broadband gateway..... | 10 |
| mobile network..... | 10 |
| PLP | |
| mapping to QCI values..... | 262 |
| mapping to traffic classes..... | 263 |
| policer action | |
| configuring | |
| for AMBR..... | 267 |
| for GBR..... | 269 |
| for MBR..... | 269 |
| overview..... | 248 |
| policer configuration | |
| exceed-action..... | 248 |
| overview..... | 248 |
| violate-action..... | 248 |
| policies | |
| configuring on broadband gateway..... | 11 |
| pool statement | |
| APN..... | 590 |
| pool-name statement | |
| APN..... | 591 |
| dhcp..... | 520 |
| pool-prefetch-threshold statement | |
| mobile pools..... | 509 |
| pool-snmp-trap-threshold statement | |
| mobile pools..... | 510 |
| preemption | |
| capability..... | 244 |
| enabling..... | 256 |
| enabling..... | 256 |
| overview..... | 244 |
| PCI flags..... | 244 |
| PVI flags..... | 244 |
| vulnerability..... | 244, 256 |
| preemption statement | |
| MobileNext Broadband Gateway..... | 719 |
| primary-list statement..... | 546 |
| priority statement | |
| dhcp..... | 521 |

| | |
|-----------------------------------|-----|
| profile statement | |
| service selection profiles..... | 613 |
| profile-id statement..... | 665 |
| profile-name statement | |
| APN..... | 592 |
| profile-selection-order statement | |
| APN..... | 593 |
| PVI flags..... | 244 |

Q

| | |
|---|----------|
| QCI | |
| configuring..... | 262 |
| overview..... | 242 |
| QoS | |
| class identifiers..... | 242 |
| configuration example..... | 277 |
| configuring | |
| local policies..... | 273 |
| configuring on Broadband Gateway | |
| overview..... | 253 |
| Differentiated Services model..... | 240 |
| initial level assigned to bearer..... | 240 |
| local policy | |
| applying at apn level..... | 274 |
| applying at system level..... | 274 |
| NQN flags and upgrade behavior..... | 251 |
| overview..... | 240 |
| traffic classes..... | 241 |
| upgrade flags and upgrade behavior..... | 251 |
| QoS Class Identifier See QCI | |
| QoS classifier profiles | |
| configuring | |
| 3G/4G networks..... | 264 |
| QoS local policy profiles | |
| APN configuration..... | 93 |
| QoS profiles | |
| configuring | |
| classifier profile..... | 264 |
| classifier profile, in 3G networks..... | 263 |
| classifier profile, in 4G networks..... | 262 |
| CoS policy profile..... | 270 |
| CoS policy profile, in 3G | |
| networks..... | 266, 268 |
| local policy..... | 273 |
| resource threshold profile..... | 260 |
| resource threshold profile, in 3G | |
| networks..... | 258 |
| resource threshold profile, in 4G | |
| networks..... | 256 |

| | |
|--------------------------------|-----|
| qos-class-identifier statement | |
| cos-cac..... | 720 |
| Quality of service See QoS | |

R

| | |
|---|------------|
| RADIUS attributes..... | 114 |
| excluding or ignoring in RADIUS | |
| messages..... | 146 |
| supported in Access-Accept messages..... | 119 |
| supported in Access-Requests..... | 115 |
| supported in Accounting On messages..... | 135 |
| supported in Accounting Start messages..... | 122 |
| supported in Accounting Stop messages..... | 131 |
| supported in CoA messages..... | 137 |
| supported in Disconnect Request | |
| messages..... | 136 |
| supported in Interim-Update messages..... | 126 |
| RADIUS options..... | 114 |
| specifying in AAA profile..... | 150 |
| RADIUS servers | |
| assigning to network elements..... | 142 |
| configuration example..... | 155 |
| configuring..... | 139 |
| enabling dynamic requests..... | 141 |
| radius statement..... | 490 |
| range statement | |
| mobile pools..... | 511 |
| reachable-time statement | |
| IPv6 router advertisement..... | 741 |
| reconnect-time statement | |
| gtp..... | 666 |
| redirect-peer statement | |
| service selection profiles..... | 614 |
| redistribute-all-traffic statement | |
| aggregated multiservices..... | 547 |
| redundancy | |
| anchor failover..... | 56 |
| broadband gateway..... | 50, 51, 52 |
| configuration example..... | 58 |
| configuring session DPC..... | 52, 54 |
| redundancy configuration example | |
| broadband gateway..... | 58 |
| rejecting | |
| maximum active bearers..... | 254 |
| rejoin-timeout statement | |
| aggregated multiservices..... | 548 |
| request interface load-balancing revert (aggregated | |
| multiservices)..... | 834 |

| | | | |
|--|-----|--|--------|
| request interface load-balancing switchover (aggregated multiservices)..... | 835 | rewrite rules | |
| request system storage unified-edge charging media start command..... | 881 | default DSCP marking | 276 |
| request system storage unified-edge charging media stop command..... | 882 | egress | |
| request system storage unified-edge media eject command..... | 883 | applying to mobile interfaces..... | 276 |
| request system storage unified-edge media prepare command..... | 884 | configuring..... | 275 |
| resource management | | overview..... | 249 |
| traceoptions..... | 18 | ingress | |
| resource threshold profiles | | applying to mobile interfaces..... | 276 |
| configuring | | configuring..... | 274 |
| in 3G networks..... | 258 | overview..... | 249 |
| in 3G/4G networks..... | 260 | overview..... | 249 |
| in 4G networks..... | 256 | rewrite-rules statement | |
| resource thresholds | | class-of-service..... | 723 |
| default settings..... | 247 | roamer-classifier-profile statement | |
| managing load | | local policies..... | 723 |
| bearer..... | 246 | roamer-cos-policy-profile statement | |
| CPU..... | 246 | local-policies..... | 724 |
| memory..... | 246 | roamer-profile statement | |
| system..... | 246 | APN..... | 595 |
| overview | 246 | roaming users | |
| preempting bearers..... | 246 | mobile network..... | 10 |
| resource-management statement..... | 794 | route lookup | |
| resource-threshold-profile statement | | GTP-C messages..... | 185 |
| cos-cac..... | 721 | router advertisement | |
| local-policies..... | 722 | IPv6 and broadband gateway..... | 67, 68 |
| restart counters..... | 183 | router solicitation | |
| restriction value | | IPv6 and broadband gateway..... | 67, 68 |
| APN configuration..... | 87 | router-lifetime statement | |
| restriction-value statement | | IPv6 router advertisement..... | 743 |
| APN..... | 594 | routing-instance statement | |
| retransmission-attempt statement | | APN..... | 596 |
| dhcp..... | 522 | gtp statement..... | 765 |
| retransmission-interval statement | | | |
| dhcp..... | 523 | S | |
| retransmission-timer statement | | s5 interface | |
| IPv6 router advertisement..... | 742 | configuring GTP services | |
| retry statement..... | 492 | for GGSN/P-GW..... | 193 |
| revert-interval statement..... | 492 | s5 statement | |
| | | gtp statement..... | 766 |
| | | s8 interface | |
| | | configuring GTP services | |
| | | for GGSN/P-GW..... | 195 |
| | | s8 statement | |
| | | gtp statement..... | 767 |
| | | secondary statement | |
| | | aggregated Packet Forwarding Engine..... | 549 |
| | | secret statement..... | 493 |

| | | | |
|--|-----|--|------|
| selection-mode statement | | show services nat pool command | |
| APN..... | 597 | aggregated multiservices..... | 991 |
| send-accounting-on statement..... | 493 | show services nat statistics command..... | 994 |
| sequence-number-length statement | | show services service-sets summary | |
| gtp statement..... | 768 | command..... | 1003 |
| server statement | | show services sessions command | |
| dhcp..... | 524 | aggregated multiservices..... | 1005 |
| resource management..... | 795 | show unified edge ggsn pgw gtp peer | |
| servers statement..... | 494 | command..... | 976 |
| service selection | | show unified edge ggsn pgw gtp statistics | |
| APN configuration..... | 97 | command..... | 974 |
| service-mode statement | | show unified edge ggsn pgw qos statistics..... | 958 |
| APN..... | 598 | show unified-edge ggsn-pgw aaa network element | |
| charging-profiles | | status command..... | 816 |
| charging..... | 667 | show unified-edge ggsn-pgw aaa network | |
| gateway..... | 749 | element-group status command..... | 814 |
| mobile pools..... | 512 | show unified-edge ggsn-pgw aaa radius statistics | |
| transport-profiles | | command..... | 817 |
| charging..... | 669 | show unified-edge ggsn-pgw aaa statistics | |
| service-selection-profile statement | | accounting command..... | 819 |
| APN..... | 599 | show unified-edge ggsn-pgw aaa statistics | |
| service-selection-profiles statement..... | 615 | authentication command..... | 821 |
| service-set statement | | show unified-edge ggsn-pgw aaa statistics | |
| aggregated multiservices..... | 776 | dynamic-requests command..... | 823 |
| services statement | | show unified-edge ggsn-pgw address-assignment | |
| dhcp..... | 525 | group command..... | 825 |
| session DPC | | show unified-edge ggsn-pgw address-assignment | |
| anchors..... | 45 | pool command..... | 827 |
| broadband gateway..... | 39 | show unified-edge ggsn-pgw address-assignment | |
| configuring..... | 40 | service-mode command..... | 829 |
| redundancy configuration..... | 52 | show unified-edge ggsn-pgw address-assignment | |
| session DPC configuration example | | statistics command..... | 831 |
| broadband gateway..... | 43 | show unified-edge ggsn-pgw apn service-mode | |
| session DPC redundancy configuration example | | command..... | 851 |
| broadband gateway..... | 58 | show unified-edge ggsn-pgw apn statistics | |
| session status..... | 355 | command..... | 854 |
| session-timeout statement | | show unified-edge ggsn-pgw call-rate statistics | |
| APN..... | 600 | command..... | 1014 |
| sgsn-sgw-change-limit statement..... | 670 | show unified-edge ggsn-pgw charging | |
| show interfaces anchor-group command | | local-persistent-storage statistics | |
| aggregated Packet Forwarding Engine..... | 836 | command..... | 885 |
| show interfaces load-balancing command | | show unified-edge ggsn-pgw charging path | |
| aggregated multiservices..... | 839 | statistics command..... | 890 |
| show services flows command | | show unified-edge ggsn-pgw charging path status | |
| aggregated multiservices..... | 982 | command..... | 930 |
| show services nat mappings app command..... | 986 | show unified-edge ggsn-pgw charging service-mode | |
| show services nat mappings eim command..... | 988 | command..... | 932 |
| show services nat mappings summary | | show unified-edge ggsn-pgw charging transfer | |
| command..... | 990 | statistics command..... | 935 |

| | | | |
|--|--------|---|-------|
| show unified-edge ggsn-pgw charging transfer status command..... | 946 | system-load statement cos-cac..... | 725 |
| show unified-edge ggsn-pgw charging trigger-profile command..... | 954 | T | |
| show unified-edge ggsn-pgw exception-handling statistics command..... | 966 | t3-response statement gtp statement..... | 768 |
| show unified-edge ggsn-pgw gateway service-mode command..... | 858 | gtp..... | 673 |
| show unified-edge ggsn-pgw ip-reassembly statistics command..... | 970 | tariff-time-list statement..... | 674 |
| show unified-edge ggsn-pgw resource-manager clients command..... | 1016 | technical support contacting JTAC..... | xxxiv |
| show unified-edge ggsn-pgw statistics command..... | 860 | TEID See tunnel endpoint identifiers | |
| show unified-edge ggsn-pgw status command..... | 862 | term statement service selection profiles..... | 616 |
| show unified-edge ggsn-pgw status preemption-list command..... | 960 | then statement service selection profiles..... | 617 |
| show unified-edge ggsn-pgw subscribers command..... | 865 | time-limit statement..... | 675 |
| show unified-edge ggsn-pgw system interfaces command..... | 842 | timeout statement..... | 496 |
| software-datapath statement..... | 744 | IP reassembly..... | 745 |
| source-interface statement..... | 495 | topic1 sub-topic..... | 935 |
| gtp..... | 671 | trace options configuring for GTP..... | 207 |
| peer..... | 671 | trace-options-dhcp statement dhcp..... | 527 |
| stop-on-access-deny statement..... | 495 | traceoptions exceptions..... | 70 |
| stop-on-failure statement..... | 496 | general gateway..... | 14 |
| streaming traffic class configuring..... | 263 | mobile options..... | 16 |
| description..... | 241 | resource manager..... | 18 |
| subscriber packets DSCP marking on..... | 276 | traceoptions statement charging..... | 676 |
| subscriber traffic policing..... | 248 | local-persistent-storage-options..... | 678 |
| support, technical See technical support | | exception handling..... | 746 |
| switch-back-time statement..... | 672 | mobile options..... | 798 |
| syntax conventions..... | xxxiii | MobileNext Broadband Gateway..... | 796 |
| system managing load | 246 | resource management client..... | 800 |
| system architecture broadband gateway..... | 3 | server..... | 803 |
| system load configuring..... | 256 | traceoptions-aaa statement..... | 498 |
| in 3G networks..... | 258 | traceoptions-gtp statement gtp statement..... | 769 |
| in 3G/4G networks..... | 261 | traceoptions-radius statement..... | 497 |
| in 4G networks..... | 256 | tracing operations for persistent storage..... | 223 |
| system statement..... | 550 | mobile charging..... | 233 |
| dhcp..... | 526 | mobile subscribers..... | 233 |

- traffic classes
 - background
 - configuring.....264
 - configuring.....263
 - GBR.....269
 - MBR.....268
 - conversational
 - configuring.....263
 - interactive
 - configuring.....264
 - overview.....241
 - streaming
 - configuring.....263
 - traffic handling priority
 - configuring.....264
 - traffic-class-classifier-profile statement
 - cos-cac.....726
 - traffic-class-cos-policy-profile statement
 - cos-cac.....727
 - transport profile change.....327, 339
 - transport profiles
 - configuring.....226
 - transport-profile statement.....680
 - transport-profiles statement.....681
 - transport-protocol statement
 - gtp.....682
 - trigger profile change.....329
 - trigger profiles
 - configuring.....227
 - trigger statement.....499
 - trigger-profile statement.....683
 - trigger-profiles statement.....684
 - tunnel endpoint identifiers.....185
 - route lookup.....185
 - tunnel management *See* GTP
- U**
- ul statement
 - local-policies.....728
 - UMTS *See* networks
 - unit statement
 - aggregated multiservices.....551
 - mobile interface.....791
 - uplink payload packet flow
 - broadband gateway.....7
 - user types
 - mobile network.....10
 - user-name statement.....685
 - user-session routing
 - broadband gateway.....81
- V**
- v4-address statement
 - gtp statement.....762
 - verify-source-address statement
 - APN.....601
 - version statement
 - gtp.....686
 - violate-action policer
 - configuring
 - for AMBR.....267
 - for MBR.....269
 - overview.....248
 - violate-action statement
 - cos-cac.....728
 - visited-profile statement
 - APN.....602
 - visiting users
 - mobile network.....10
 - visitor-classifier-profile statement
 - local-policies.....729
 - visitor-cos-policy-profile statement
 - local-policies.....729
 - volume-limit statement.....687
 - VRFs
 - broadband gateway.....96
 - VSAs
 - excluding from RADIUS messages.....146
 - supported.....110
- W**
- wait-accounting statement
 - APN.....603
 - configuring.....152
 - warm-standby statement
 - aggregated Packet Forwarding Engine.....552
 - watermark-level-1 statement.....688
 - watermark-level-2 statement.....689
 - watermark-level-3 statement.....690
 - world-readable statement.....691

Index of Statements and Commands

A

| | |
|---|-----|
| aaa statement..... | 470 |
| APN..... | 553 |
| aaa-override statement | |
| APN..... | 554 |
| aaa-profile statement | |
| APN..... | 555 |
| aaa-radius statement..... | 488 |
| accounting statement | |
| unified-edge profile..... | 472 |
| accounting-port statement..... | 473 |
| accounting-secret statement..... | 473 |
| address statement..... | 474 |
| address-assignment statement | |
| APN..... | 556 |
| MobileNext Broadband Gateway..... | 502 |
| ageing-window statement | |
| mobile pools..... | 503 |
| aggregated-maximum-bit-rate statement | |
| cos-cac..... | 693 |
| algorithm statement..... | 474 |
| allocation and retention-priority statement | |
| cos-cac..... | 694 |
| allow-dynamic-requests statement..... | 475 |
| allow-static-ip-address statement | |
| APN..... | 557 |
| anchor-pfes statement..... | 529 |
| anchor-spics statement..... | 530 |
| anchoring-options statement..... | 531 |
| anonymous-user statement | |
| APN..... | 558 |
| apfe-group-set statement..... | 532 |
| apn-data-type statement | |
| APN..... | 559 |
| apn-name statement | |
| service selection profiles..... | 604 |

| | |
|------------------------------------|-----|
| apn-services statement..... | 560 |
| apn-type statement | |
| APN..... | 562 |
| apns statement..... | 563 |
| APN services..... | 563 |
| attributes statement..... | 476 |
| authentication statement..... | 477 |
| authentication-port statement..... | 477 |

B

| | |
|---------------------------------------|-----|
| bandwidth-pool statement | |
| cos-cac..... | 695 |
| bearer-load statement | |
| cos-cac..... | 696 |
| bind-interface statement | |
| dhcp..... | 513 |
| block-visitors statement | |
| APN..... | 565 |
| broadband gateway | |
| interface redundancy..... | 52 |
| interfaces redundancy configuration | |
| example..... | 58 |
| redundancy configuration..... | 50 |
| redundancy configuration example..... | 58 |
| Routing Engine redundancy..... | 50 |
| session DPC redundancy..... | 51 |
| session DPC redundancy configuration | |
| example..... | 58 |

C

| | |
|--------------------------------------|--------|
| call-rate-statistics statement..... | 779 |
| cdr-aggregation-limit statement..... | 619 |
| cdr-profile statement..... | 620 |
| cdr-profiles statement..... | 621 |
| cdr-release statement | |
| charging-gateways..... | 622 |
| cdrs-per-file statement..... | 623 |
| charging statement..... | 624 |
| APN..... | 566 |
| charging-characteristics statement | |
| service selection profiles..... | 605 |
| charging-gateways statement..... | 627 |
| charging-profiles statement..... | 628 |
| chassis | |
| redundancy configuration..... | 52, 54 |
| class-of-service statement..... | 699 |
| classifier-profile statement | |
| local-policies..... | 697 |

| | | |
|--|-----|--|
| classifier-profiles statement | | |
| cos-cac..... | 698 | |
| clear unified edge ggsn pgw gtp peer statistics | | |
| command..... | 979 | |
| clear unified edge ggsn pgw gtp statistics | | |
| command..... | 978 | |
| clear unified-edge ggsn-pgw charging cdr | | |
| command..... | 876 | |
| clear unified-edge ggsn-pgw charging cdr wfa | | |
| command..... | 877 | |
| clear unified-edge ggsn-pgw charging | | |
| local-persistent-storage statistics | | |
| command..... | 878 | |
| clear unified-edge ggsn-pgw charging path | | |
| statistics command..... | 879 | |
| clear unified-edge ggsn-pgw charging transfer | | |
| statistics command..... | 880 | |
| clear unified-edge ggsn-pgw exception-handling | | |
| statistics command..... | 964 | |
| clear unified-edge ggsn-pgw ip-reassembly | | |
| statistics command..... | 965 | |
| clear unified-edge ggsn-pgw statistics | | |
| command..... | 846 | |
| clear unified-edge ggsn-pgw subscribers charging | | |
| command..... | 849 | |
| clear unified-edge ggsn-pgw subscribers | | |
| command..... | 847 | |
| clear unified-edge ggsn-pgw subscribers peer | | |
| command..... | 850 | |
| client statement | | |
| resource management..... | 792 | |
| configuration | | |
| broadband gateway interface PFEs..... | 50 | |
| broadband gateway services PICs..... | 50 | |
| configuration example | | |
| redundancy..... | 58 | |
| configuring chassis | | |
| interfaces for mobility redundancy..... | 54 | |
| session DPC redundancy..... | 52 | |
| configuring interfaces for mobility | | |
| redundancy..... | 54 | |
| configuring redundancy | | |
| interfaces for mobility..... | 54 | |
| session DPC..... | 52 | |
| configuring session DPC | | |
| redundancy..... | 52 | |
| container-limit statement..... | 629 | |
| control statement | | |
| gtp statement..... | 751 | |
| cos-cac statement..... | 700 | |
| cos-policy-profile statement | | |
| local-policies..... | 702 | |
| cos-policy-profiles statement | | |
| cos-cac..... | 703 | |
| cpu statement | | |
| cos-cac..... | 704 | |
| current-hop-limit statement | | |
| IPv6 router advertisement..... | 731 | |
| D | | |
| data statement | | |
| gtp statement..... | 752 | |
| dead-criteria-retries statement..... | 478 | |
| dead-server-retry-interval statement | | |
| dhcp..... | 514 | |
| dead-server-successive-retry-attempt statement | | |
| dhcp..... | 515 | |
| default-pool statement | | |
| mobile pools..... | 503 | |
| default-profile statement | | |
| APN..... | 567 | |
| default-rating-group statement..... | 629 | |
| default-service-id statement..... | 630 | |
| description statement | | |
| APN..... | 568 | |
| cdr-profiles..... | 631 | |
| charging-profiles..... | 631 | |
| transport-profiles..... | 631 | |
| trigger-profiles..... | 631 | |
| destination-ipv4-address statement..... | 632 | |
| destination-port statement | | |
| gtp..... | 633 | |
| DHCP | | |
| configuring..... | 168 | |
| APN..... | 169 | |
| dhcp-proxy-client statement | | |
| APN..... | 569 | |
| dhcp..... | 516 | |
| dhcp-server-selection-algorithm statement | | |
| dhcp..... | 517 | |
| dhcipv4-profiles statement | | |
| dhcp..... | 518 | |
| dhcipv4-proxy-client-profile statement | | |
| APN..... | 570 | |
| dhcipv6-profiles statement | | |
| dhcp..... | 519 | |
| dhcipv6-proxy-client-profile statement | | |
| APN..... | 571 | |

| | | | |
|---|-----|--|-----|
| direction statement..... | 634 | exclude-v6pools statement | |
| disable statement | | APN..... | 574 |
| IPv6 router advertisement..... | 732 | external-assigned statement | |
| disable-replication statement..... | 635 | mobile pools..... | 504 |
| disk-space-policy statement..... | 636 | F | |
| dl-bandwidth-pool statement | | family statement | |
| local-policies..... | 705 | aggregated multiservices..... | 535 |
| dns-server statement | | mobile interface..... | 780 |
| APN..... | 572 | mobile pools..... | 505 |
| down-detect-time statement | | file-age statement..... | 646 |
| gtp..... | 637 | file-creation-policy statement..... | 647 |
| drop-member-traffic statement | | file-format statement..... | 648 |
| aggregated multiservices..... | 533 | file-name-private-extension statement..... | 649 |
| dscp-code-point statement | | file-size statement..... | 650 |
| gtp statement..... | 752 | filter statement | |
| dscp-ipv6-rewrite-rule-name statement | | mobile interface..... | 780 |
| class-of-service..... | 705 | forwarding-class statement | |
| dscp-ipv6-rewrite-rule-name-ingress statement | | gtp statement..... | 755 |
| class-of-service..... | 706 | forwarding-packages statement..... | 781 |
| dscp-rewrite-rule-name statement | | from statement | |
| class-of-service..... | 706 | service selection profiles..... | 606 |
| dscp-rewrite-rule-name-ingress statement | | G | |
| class-of-service..... | 707 | ggsn-pgw statement..... | 782 |
| dynamic-requests-secret statement..... | 478 | gn statement | |
| E | | gtp statement..... | 756 |
| echo interval | | gp statement | |
| gtp..... | 753 | gtp statement..... | 757 |
| echo-interval statement | | group statement | |
| gtp..... | 638 | APN..... | 575 |
| echo-n3-requests statement | | gtp statement | |
| gtp statement..... | 753 | gtp statement..... | 758 |
| echo-t3-response statement | | gtp statement..... | 651 |
| gtp statement..... | 754 | guaranteed-bit-rate statement | |
| egress-key statement | | cos-cac..... | 708 |
| aggregated multiservices..... | 771 | H | |
| enable-reduced-partial-cdrs statement..... | 639 | hash-keys statement | |
| enable-rejoin statement | | aggregated multiservices..... | 772 |
| aggregated multiservices..... | 534 | header-type statement | |
| error-indication-interval statement..... | 732 | gtp..... | 652 |
| gtp statement..... | 754 | high statement | |
| exceed-action statement | | cos-cac..... | 709 |
| cos-cac..... | 707 | high-availability-options statement | |
| exclude statement..... | 479 | aggregated multiservices..... | 536 |
| trigger-profiles..... | 640 | history statement | |
| exclude-ie-options statement..... | 642 | call-rate statistics..... | 782 |
| exclude-pools statement | | home-plmn statement..... | 783 |
| APN..... | 573 | | |

| | | |
|---|----------|--|
| home-profile statement | | |
| APN..... | 576 | |
| I | | |
| idle-timeout statement | | |
| APN..... | 577 | |
| idle-timeout-direction statement | | |
| APN..... | 578 | |
| ignore statement..... | 481 | |
| imei statement | | |
| service selection profiles..... | 607 | |
| imsi statement | | |
| service selection profiles..... | 608 | |
| inet-pool statement | | |
| APN..... | 579 | |
| inet-precedence-rewrite-rule-name statement | | |
| class-of-service..... | 709 | |
| inet-precedence-rewrite-rule-name-ingress statement | | |
| class-of-service..... | 710 | |
| inet6-pool statement | | |
| APN..... | 580 | |
| ingress-key statement | | |
| aggregated multiservices..... | 773 | |
| ingress-rewrite-rules statement | | |
| class of service..... | 710 | |
| input statement | | |
| mobile interface..... | 783 | |
| inter-mobile-traffic statement | | |
| APN..... | 581 | |
| interface redundancy configuration example | | |
| broadband gateway..... | 58 | |
| interface statement..... | 784 | |
| anchor Packet Forwarding Engine..... | 537 | |
| gtp statement..... | 761 | |
| multiservices PIC..... | 538 | |
| interface-service statement | | |
| aggregated multiservices..... | 774 | |
| interfaces for mobility | | |
| redundancy configuration..... | 54 | |
| interfaces statement | | |
| aggregated multiservices..... | 539 | |
| aggregated Packet Forwarding Engine..... | 540 | |
| class-of-service..... | 711 | |
| mobile interface..... | 785 | |
| interval statement | | |
| call-rate statistics..... | 786 | |
| ip-reassembly statement..... | 733 | |
| ip-reassembly-profile statement..... | 734 | |
| ipv6-router-advertisement statement..... | 735 | |
| L | | |
| lease-time statement | | |
| dhcp..... | 520 | |
| load-balancing-options statement | | |
| aggregated multiservices..... | 541, 775 | |
| local statement | | |
| APN..... | 582 | |
| local-persistent-storage-options statement..... | 653 | |
| local-policies..... | 712 | |
| local-policy-profile statement | | |
| APN..... | 583 | |
| MobileNext Broadband Gateway..... | 713 | |
| local-storage statement..... | 654 | |
| logical-system statement | | |
| APN..... | 584 | |
| low statement | | |
| cos-cac..... | 714 | |
| M | | |
| many-to-one statement | | |
| aggregated multiservices..... | 542 | |
| max-reassembly-pending-packets statement | | |
| IP reassembly..... | 736 | |
| maximum-advertisement-interval statement | | |
| IPv6 router advertisement..... | 737 | |
| maximum-bearers statement | | |
| APN..... | 585 | |
| MobileNext Broadband Gateway..... | 715 | |
| service selection profiles..... | 609 | |
| maximum-bit-rate statement | | |
| cos-cac..... | 716 | |
| maximum-initial-advertisement-interval statement | | |
| IPv6 router advertisement..... | 738 | |
| maximum-initial-advertisements statement | | |
| IPv6 router advertisement..... | 739 | |
| maximum-pending-reqs-limit statement..... | 481 | |
| mcc statement..... | 787 | |
| member-failure-options statement | | |
| aggregated multiservices..... | 543 | |
| member-interface statement | | |
| aggregated multiservices..... | 545 | |
| memory statement | | |
| cos-cac..... | 717 | |
| mif statement | | |
| class of service..... | 718 | |
| minimum-advertisement-interval statement | | |
| IPv6 router advertisement..... | 740 | |

| | | | |
|---------------------------------------|-----|---|-----|
| mnc statement..... | 788 | pdn-type statement | |
| mobile options statement..... | 793 | service selection profiles..... | 611 |
| mobile-interface statement | | peer statement | |
| APN..... | 586 | gtp statement..... | 763 |
| mobile-pool-groups statement..... | 506 | gtp..... | 660 |
| mobile-pools statement..... | 507 | peer-order..... | 661 |
| mobile-profiles statement..... | 482 | service selection profiles..... | 611 |
| mobility statement..... | 789 | peer-group statement | |
| msisdn statement | | gtp statement..... | 764 |
| service selection profiles..... | 610 | peer-history statement | |
| mtu statement..... | 655 | gtp statement..... | 765 |
| mobile interface..... | 790 | peer-order statement..... | 662 |
| | | peer-routing-instance statement | |
| N | | service selection profiles..... | 612 |
| n3-requests statement | | pending-queue-size statement | |
| gtp statement..... | 762 | gtp..... | 663 |
| gtp..... | 656 | persistent-storage-order statement..... | 664 |
| nbns-server statement | | pool statement | |
| APN..... | 587 | APN..... | 590 |
| network statement | | pool-name statement | |
| mobile pools..... | 508 | APN..... | 591 |
| network-element statement..... | 484 | dhcp..... | 520 |
| network-element-group statement..... | 484 | pool-prefetch-threshold statement | |
| network-element-groups statement..... | 485 | mobile pools..... | 509 |
| network-elements statement..... | 486 | pool-snmp-trap-threshold statement | |
| no-address-verify statement | | mobile pools..... | 510 |
| APN..... | 588 | preemption statement | |
| no-path-management statement | | MobileNext Broadband Gateway..... | 719 |
| gtp..... | 657 | primary-list statement..... | 546 |
| | | priority statement | |
| O | | dhcp..... | 521 |
| offline statement | | profile statement | |
| transport-profiles..... | 658 | service selection profiles..... | 613 |
| trigger-profiles..... | 659 | profile-id statement..... | 665 |
| options statement | | profile-name statement | |
| RADIUS..... | 487 | APN..... | 592 |
| output statement | | profile-selection-order statement | |
| mobile interface..... | 790 | APN..... | 593 |
| overview | | | |
| interface redundancy..... | 52 | Q | |
| Routing Engine redundancy..... | 50 | qos-class-identifier statement | |
| session DPC redundancy..... | 51 | cos-cac..... | 720 |
| | | | |
| P | | R | |
| p-cscf statement | | radius statement..... | 490 |
| APN..... | 589 | range statement | |
| path-management statement | | mobile pools..... | 511 |
| gtp statement..... | 763 | reachable-time statement | |
| | | IPv6 router advertisement..... | 741 |

| | |
|---|------------|
| reconnect-time statement | |
| gtp..... | 666 |
| redirect-peer statement | |
| service selection profiles..... | 614 |
| redistribute-all-traffic statement | |
| aggregated multiservices..... | 547 |
| redundancy | |
| broadband gateway..... | 50, 51, 52 |
| configuration example..... | 58 |
| configuring session DPC..... | 52, 54 |
| redundancy configuration example | |
| broadband gateway..... | 58 |
| rejoin-timeout statement | |
| aggregated multiservices..... | 548 |
| request interface load-balancing revert (aggregated multiservices)..... | 834 |
| request interface load-balancing switchover (aggregated multiservices)..... | 835 |
| request system storage unified-edge charging media start command..... | 881 |
| request system storage unified-edge charging media stop command..... | 882 |
| request system storage unified-edge media eject command..... | 883 |
| request system storage unified-edge media prepare command..... | 884 |
| resource-management statement..... | 794 |
| resource-threshold-profile statement | |
| cos-cac..... | 721 |
| local-policies..... | 722 |
| restriction-value statement | |
| APN..... | 594 |
| retransmission-attempt statement | |
| dhcp..... | 522 |
| retransmission-interval statement | |
| dhcp..... | 523 |
| retransmission-timer statement | |
| IPv6 router advertisement..... | 742 |
| retry statement..... | 492 |
| revert-interval statement..... | 492 |
| rewrite-rules statement | |
| class-of-service..... | 723 |
| roamer-classifier-profile statement | |
| local policies..... | 723 |
| roamer-cos-policy-profile statement | |
| local-policies..... | 724 |
| roamer-profile statement | |
| APN..... | 595 |
| router-lifetime statement | |
| IPv6 router advertisement..... | 743 |
| routing-instance statement | |
| APN..... | 596 |
| gtp statement..... | 765 |
| S | |
| s5 statement | |
| gtp statement..... | 766 |
| s8 statement | |
| gtp statement..... | 767 |
| secondary statement | |
| aggregated Packet Forwarding Engine..... | 549 |
| secret statement..... | 493 |
| selection-mode statement | |
| APN..... | 597 |
| send-accounting-on statement..... | 493 |
| sequence-number-length statement | |
| gtp statement..... | 768 |
| server statement | |
| dhcp..... | 524 |
| resource management..... | 795 |
| servers statement..... | 494 |
| service-mode statement | |
| APN..... | 598 |
| charging-profiles | |
| charging..... | 667 |
| gateway..... | 749 |
| mobile pools..... | 512 |
| transport-profiles | |
| charging..... | 669 |
| service-selection-profile statement | |
| APN..... | 599 |
| service-selection-profiles statement..... | 615 |
| service-set statement | |
| aggregated multiservices..... | 776 |
| services statement | |
| dhcp..... | 525 |
| session DPC | |
| redundancy configuration..... | 52 |
| session DPC redundancy configuration example | |
| broadband gateway..... | 58 |
| session-timeout statement | |
| APN..... | 600 |
| sgsn-sgw-change-limit statement..... | 670 |
| show interfaces anchor-group command | |
| aggregated Packet Forwarding Engine..... | 836 |
| show interfaces load-balancing command | |
| aggregated multiservices..... | 839 |

| | | | |
|--|------|---|------|
| show services flows command | | show unified-edge ggsn-pgw charging path status | |
| aggregated multiservices..... | 982 | command..... | 930 |
| show services nat mappings app command..... | 986 | show unified-edge ggsn-pgw charging service-mode | |
| show services nat mappings eim command..... | 988 | command..... | 932 |
| show services nat mappings summary | | show unified-edge ggsn-pgw charging transfer | |
| command..... | 990 | statistics command..... | 935 |
| show services nat pool command | | show unified-edge ggsn-pgw charging transfer | |
| aggregated multiservices..... | 991 | status command..... | 946 |
| show services nat statistics command..... | 994 | show unified-edge ggsn-pgw charging | |
| show services service-sets summary | | trigger-profile command..... | 954 |
| command..... | 1003 | show unified-edge ggsn-pgw exception-handling | |
| show services sessions command | | statistics command..... | 966 |
| aggregated multiservices..... | 1005 | show unified-edge ggsn-pgw gateway | |
| show unified edge ggsn pgw gtp peer | | service-mode command..... | 858 |
| command..... | 976 | show unified-edge ggsn-pgw ip-reassembly | |
| show unified edge ggsn pgw gtp statistics | | statistics command..... | 970 |
| command..... | 974 | show unified-edge ggsn-pgw resource-manager | |
| show unified edge ggsn pgw qos statistics..... | 958 | clients command..... | 1016 |
| show unified-edge ggsn-pgw aaa network element | | show unified-edge ggsn-pgw statistics | |
| status command..... | 816 | command..... | 860 |
| show unified-edge ggsn-pgw aaa network | | show unified-edge ggsn-pgw status | |
| element-group status command..... | 814 | command..... | 862 |
| show unified-edge ggsn-pgw aaa radius statistics | | show unified-edge ggsn-pgw status preemption-list | |
| command..... | 817 | command..... | 960 |
| show unified-edge ggsn-pgw aaa statistics | | show unified-edge ggsn-pgw subscribers | |
| accounting command..... | 819 | command..... | 865 |
| show unified-edge ggsn-pgw aaa statistics | | show unified-edge ggsn-pgw system interfaces | |
| authentication command..... | 821 | command..... | 842 |
| show unified-edge ggsn-pgw aaa statistics | | software-datapath statement..... | 744 |
| dynamic-requests command..... | 823 | source-interface statement..... | 495 |
| show unified-edge ggsn-pgw address-assignment | | gtp..... | 671 |
| group command..... | 825 | peer..... | 671 |
| show unified-edge ggsn-pgw address-assignment | | stop-on-access-deny statement..... | 495 |
| pool command..... | 827 | stop-on-failure statement..... | 496 |
| show unified-edge ggsn-pgw address-assignment | | switch-back-time statement..... | 672 |
| service-mode command..... | 829 | system statement..... | 550 |
| show unified-edge ggsn-pgw address-assignment | | dhcp..... | 526 |
| statistics command..... | 831 | system-load statement | |
| show unified-edge ggsn-pgw apn service-mode | | cos-cac..... | 725 |
| command..... | 851 | | |
| show unified-edge ggsn-pgw apn statistics | | T | |
| command..... | 854 | t3-response statement | |
| show unified-edge ggsn-pgw call-rate statistics | | gtp statement..... | 768 |
| command..... | 1014 | gtp..... | 673 |
| show unified-edge ggsn-pgw charging | | tariff-time-list statement..... | 674 |
| local-persistent-storage statistics | | term statement | |
| command..... | 885 | service selection profiles..... | 616 |
| show unified-edge ggsn-pgw charging path | | then statement | |
| statistics command..... | 890 | service selection profiles..... | 617 |

| | |
|--|-----|
| time-limit statement..... | 675 |
| timeout statement..... | 496 |
| IP reassembly..... | 745 |
| trace-options-dhcp statement | |
| dhcp..... | 527 |
| traceoptions statement | |
| charging..... | 676 |
| local-persistent-storage-options..... | 678 |
| exception handling..... | 746 |
| mobile options..... | 798 |
| MobileNext Broadband Gateway..... | 796 |
| resource management | |
| client..... | 800 |
| server..... | 803 |
| traceoptions-aaa statement..... | 498 |
| traceoptions-gtp statement | |
| gtp statement..... | 769 |
| traceoptions-radius statement..... | 497 |
| traffic-class-classifier-profile statement | |
| cos-cac..... | 726 |
| traffic-class-cos-policy-profile statement | |
| cos-cac..... | 727 |
| transport-profile statement..... | 680 |
| transport-profiles statement..... | 681 |
| transport-protocol statement | |
| gtp..... | 682 |
| trigger statement..... | 499 |
| trigger-profile statement..... | 683 |
| trigger-profiles statement..... | 684 |

U

| | |
|-------------------------------|-----|
| ul statement | |
| local-policies..... | 728 |
| unit statement | |
| aggregated multiservices..... | 551 |
| mobile interface..... | 791 |
| user-name statement..... | 685 |

V

| | |
|---------------------------------|-----|
| v4-address statement | |
| gtp statement..... | 762 |
| verify-source-address statement | |
| APN..... | 601 |
| version statement | |
| gtp..... | 686 |
| violate-action statement | |
| cos-cac..... | 728 |
| visited-profile statement | |
| APN..... | 602 |

| | |
|--------------------------------------|-----|
| visitor-classifier-profile statement | |
| local-policies..... | 729 |
| visitor-cos-policy-profile statement | |
| local-policies..... | 729 |
| volume-limit statement..... | 687 |

W

| | |
|--|-----|
| wait-accounting statement | |
| APN..... | 603 |
| warm-standby statement | |
| aggregated Packet Forwarding Engine..... | 552 |
| watermark-level-1 statement..... | 688 |
| watermark-level-2 statement..... | 689 |
| watermark-level-3 statement..... | 690 |
| world-readable statement..... | 691 |