

# MobileNext Broadband Gateway

## Monitoring and Troubleshooting Guide

Release  
**12.1**



Published: 2013-03-12

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA  
408-745-2000  
www.juniper.net

Copyright © 2013, Juniper Networks, Inc. All rights reserved.

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 Monitoring and Troubleshooting Guide*

Copyright © 2013, Juniper Networks, Inc.

All rights reserved.

Revision History

February 2013—R2 Junos OS 12.1W

The information in this document is current as of the date on the title page.

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.

# Table of Contents

	<b>About This Guide . . . . .</b>	<b>v</b>
	Junos Documentation and Release Notes . . . . .	v
	Objectives . . . . .	v
	Audience . . . . .	vi
	Supported Platforms . . . . .	vi
	Documentation Conventions . . . . .	vi
	Documentation Feedback . . . . .	viii
	Requesting Technical Support . . . . .	viii
	Self-Help Online Tools and Resources . . . . .	ix
	Opening a Case with JTAC . . . . .	ix
<b>Part 1</b>	<b>Monitoring</b>	
<b>Chapter 1</b>	<b>Monitoring . . . . .</b>	<b>3</b>
	Monitoring the Mobile Environment—Key Performance Indicators . . . . .	3
	Monitoring Resources . . . . .	4
	Monitoring GTP Signaling . . . . .	4
	Monitoring Session Status . . . . .	6
	Monitoring CPU Indicators . . . . .	6
	Monitoring Memory Indicators . . . . .	7
	Monitoring Charging Gateways . . . . .	7
	Monitoring Data Path Measurements . . . . .	9
	Monitoring Call-Rate Statistics . . . . .	9
	Monitoring Data Rate Statistics . . . . .	10
	Call Trace Overview . . . . .	11
	Example: Monitoring a P-GW with Call Trace . . . . .	12
	Example: Monitoring an S-GW with Call Trace . . . . .	14
<b>Part 2</b>	<b>Troubleshooting</b>	
<b>Chapter 2</b>	<b>Troubleshooting . . . . .</b>	<b>19</b>
	Troubleshooting Mobility Overview . . . . .	19
	Request Support Information Overview . . . . .	20
	Troubleshooting Overload Conditions in the Mobile Network . . . . .	20
	Troubleshooting Multilevel Overload Protection . . . . .	21
	Responding to an Overload . . . . .	21
	Monitoring GTP Signaling . . . . .	22
	Troubleshooting Call Admission Control . . . . .	23
	Monitoring AAA Metrics . . . . .	25

## Part 3

## Index

Index .....	33
-------------	----

# About This Guide

- Junos Documentation and Release Notes on page v
- Objectives on page v
- Audience on page vi
- Supported Platforms on page vi
- Documentation Conventions on page vi
- Documentation Feedback on page viii
- Requesting Technical Support on page viii

## 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 information about the mobility features of the Junos OS on the MobileNext Broadband Gateway and describes how to monitor and troubleshoot these features 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 document, the following platforms are supported:

- [MX240 Routers](#)
- [MX960 Routers](#)
- [MX480 Routers](#)

## Documentation Conventions

---

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

Table 2: Text and Syntax Conventions

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

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

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

## Documentation Feedback

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

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

## Requesting Technical Support

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



or are covered under warranty, and need post-sales 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/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- 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, see <http://www.juniper.net/support/requesting-support.html>.



## PART 1

# Monitoring

- [Monitoring on page 3](#)



## CHAPTER 1

# Monitoring

- [Monitoring the Mobile Environment—Key Performance Indicators on page 3](#)
- [Monitoring Resources on page 4](#)
- [Monitoring GTP Signaling on page 4](#)
- [Monitoring Session Status on page 6](#)
- [Monitoring CPU Indicators on page 6](#)
- [Monitoring Memory Indicators on page 7](#)
- [Monitoring Charging Gateways on page 7](#)
- [Monitoring Data Path Measurements on page 9](#)
- [Monitoring Call-Rate Statistics on page 9](#)
- [Monitoring Data Rate Statistics on page 10](#)
- [Call Trace Overview on page 11](#)
- [Example: Monitoring a P-GW with Call Trace on page 12](#)
- [Example: Monitoring an S-GW with Call Trace on page 14](#)

### **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 OS Mobility environment.

These key performance indicators include the following:

- GTP signaling statistics
- Session status indicators
- CPU utilization indicators
- Memory utilization indicators
- Monitored resource usage indicators (address pools, gateway and APN bandwidth usage, Packet Forwarding Engine load, and so on)
- Authentication or accounting (AAA) metrics
- Charging gateway status and congestion indicators with round trip time calculations
- Data path measurements

- Per server statistics for AAA, GTP, and the charging gateway
- Data rate measurements per configured interval

**Related  
Documentation**

- [Monitoring Data Path Measurements on page 9](#)
- [Monitoring Data Rate Statistics on page 10](#)
- [Monitoring GTP Signaling on page 4](#)
- [Monitoring Session Status on page 6](#)

## Monitoring Resources

---

To avoid overload conditions, monitor the following resources:

- Detailed control plane snapshot of the 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
- Average load on individual session PICs
- System data path bandwidth for assured quality of service
- Queue depths (AAA, charging, GTP input, and so on)
- External interfaces like RADIUS and charging gateway by tracking success and failure statistics, monitoring round trip time, and so on
- Internal resource usage for local pool addresses available and so on

**Related  
Documentation**

- [Monitoring AAA Metrics on page 25](#)
- [Monitoring the Mobile Environment—Key Performance Indicators on page 3](#)
- [Request Support Information Overview on page 20](#)

## 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 the following:

- Per peer history
- Per GTP cause code statistics for granular measurement of the number of failures

- Separate session establishments attempts and 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, execute the following command:

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

For more information, see the *show unified-edge ggsn-pgw resource-manager clients* topic in the *MobileNext Broadband Gateway Statements and Commands Reference Guide*.

2. To see a summary of subscribers on the gateway, execute the following command:

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

For more information, see the *show unified-edge ggsn-pgw status* topic in the *MobileNext Broadband Gateway Statements and Commands Reference Guide*.

3. To see subscriber details, execute the following command:

```
user@host> show unified-edge ggsn-pgw subscribers extensive
```

For more information, see the *show unified-edge ggsn-pgw subscribers* topic in the *MobileNext Broadband Gateway Statements and Commands Reference Guide*.

4. To see all GTP statistics (including messages sent and received, and cause codes sent and received), execute the following command:

```
user@host> show unified-edge ggsn-pgw gtp statistics detail
```

For more information, see the *show unified-edge ggsn-pgw gtp statistics* topic in the *MobileNext Broadband Gateway Statements and Commands Reference Guide*.

5. To see all the GTP peers, execute the following command:

```
user@host> show unified-edge ggsn-pgw gtp peer detail
```

For more information, see the *show unified-edge ggsn-pgw gtp peer* topic in the *MobileNext Broadband Gateway Statements and Commands Reference Guide*.

#### Related Documentation

- [Monitoring AAA Metrics on page 25](#)
- [Monitoring the Mobile Environment—Key Performance Indicators on page 3](#)
- [Monitoring Resources on page 4](#)
- [Request Support Information Overview on page 20](#)
- [Responding to an Overload on page 21](#)
- [show unified-edge ggsn-pgw gtp peer](#)
- [show unified-edge ggsn-pgw gtp statistics](#)
- [show unified-edge ggsn-pgw resource-manager clients](#)
- [show unified-edge ggsn-pgw status](#)
- [show unified-edge ggsn-pgw subscribers](#)

- [Troubleshooting Call Admission Control on page 23](#)
- [Troubleshooting Mobility Overview on page 19](#)
- [Troubleshooting Multilevel Overload Protection on page 21](#)
- [Troubleshooting Overload Conditions in the Mobile Network on page 20](#)

## Monitoring Session Status

---

Current session or bearer counts can be monitored at various levels; for example, per APN, per QCI/ARP, per RAT type, per APN, per QCI, or at the global level.

To monitor the session status, do the following:

- To examine session status indicators at the APN, gateway, and other levels, execute the following command:

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

For more information, see the *show unified-edge ggsn-pgw statistics* topic in the *MobileNext Broadband Gateway Statements and Commands Reference Guide*.

- To view the statistics for the specified traffic class, execute the following command:

```
user@host> show unified-edge ggsn-pgw statistics traffic-class
```

For more information, see the *show unified-edge ggsn-pgw statistics traffic-class* topic in the *MobileNext Broadband Gateway Statements and Commands Reference Guide*.

### Related Documentation

- [Monitoring the Mobile Environment—Key Performance Indicators on page 3](#)
- [Monitoring Resources on page 4](#)
- `show unified-edge ggsn-pgw statistics`
- `show unified-edge ggsn-pgw statistics traffic-class`

## Monitoring CPU Indicators

---

Monitoring CPU utilization relies on gathering data from session PICs.

To monitor CPU utilization, do the following:

- To see the status indicators at the gateway level, execute the following command:

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

- To see status indicators for all PICs, execute the following command:

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

- To see status indicators for an individual PIC, execute the following command:

```
user@host> show unified-edge ggsn-pgw status fpc-slot fpc-slot pic-slot pic-slot
```

For example, to see the status indicators for a PIC in FPC slot 2 and PIC slot 0 enter:



```
user@host> show unified-edge ggsn-pgw status fpc-slot 2 pic-slot 0
```

For more information, see the *show unified-edge ggsn-pgw status* topic in the *MobileNext Broadband Gateway Statements and Commands Reference Guide*.

#### Related Documentation

- [Monitoring Memory Indicators on page 7](#)
- [Monitoring Resources on page 4](#)
- [Monitoring the Mobile Environment—Key Performance Indicators on page 3](#)
- `show unified-edge ggsn-pgw status`

## Monitoring Memory Indicators

You can monitor system memory by gathering data from session PICs just as you do for CPU usage.

To monitor memory utilization, do the following:

- To see the memory indicators at the gateway level, execute the following command:  

```
user@host> show unified-edge ggsn-pgw status brief
```
- To see memory indicators for all PICs, execute the following command:  

```
user@host> show unified-edge ggsn-pgw status detail
```
- To see memory indicators for an individual PIC, execute the following command:  

```
user@host> show unified-edge ggsn-pgw status fpc-slot fpc-slot pic-slot pic-slot
```

For example, to see the memory indicators for a PIC in FPC slot 2 and PIC slot 0 enter:

```
user@host> show unified-edge ggsn-pgw status fpc-slot 2 pic-slot 0
```

For more information, see the *show unified-edge ggsn-pgw status* topic in the *MobileNext Broadband Gateway Statements and Commands Reference Guide*.

#### Related Documentation

- [Monitoring CPU Indicators on page 6](#)
- [Monitoring Resources on page 4](#)
- [Monitoring the Mobile Environment—Key Performance Indicators on page 3](#)
- `show unified-edge ggsn-pgw status`

## Monitoring Charging Gateways

Charging gateways can be monitored by checking status and pending CDR counts, and per transport profile. The specific statistics you can gather for a charging gateway are as follows:

- Status (alive or dead)
- Number of echo requests transmitted, received, and number of echo requests that timed out

- 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 (DRT) requests transmitted and number of DRT requests that timed out
- Number of DRT success responses received
- Total round trip time of the previous DRT (average, maximum, and minimum)

To monitor charging gateways, do the following:

- To see the status of the configured GTP Prime (GTPP) peers, execute the following command:

```
user@host> show unified-edge ggsn-pgw charging path status
```

For more information, see the *show unified-edge ggsn-pgw charging path status* topic in the *MobileNext Broadband Gateway Statements and Commands Reference Guide*.

- To see the path management message statistics (between the Charging Data Function (CDF) and the Charging Gateway Function (CGF) servers), execute the following command:

```
user@host> show unified-edge ggsn-pgw charging path statistics
```

For more information, see the *show unified-edge ggsn-pgw charging path statistics* topic in the *MobileNext Broadband Gateway Statements and Commands Reference Guide*.

- To see the status of the Charging Data Record (CDR) transfers for the configured transport profiles, execute the following command:

```
user@host> show unified-edge ggsn-pgw charging transfer status
```

For more information, see the *show unified-edge ggsn-pgw charging transfer status* topic in the *MobileNext Broadband Gateway Statements and Commands Reference Guide*.

- To see the transfer statistics for the configured transport profiles, execute the following command:

```
user@host> show unified-edge ggsn-pgw charging transfer statistics
```

For more information, see the *show unified-edge ggsn-pgw charging transfer statistics* topic in the *MobileNext Broadband Gateway Statements and Commands Reference Guide*.

**Related  
Documentation**

- [Monitoring the Mobile Environment—Key Performance Indicators on page 3](#)
- [Monitoring Resources on page 4](#)

- show unified-edge ggsn-pgw charging path statistics
- show unified-edge ggsn-pgw charging path status
- show unified-edge ggsn-pgw charging transfer statistics
- show unified-edge ggsn-pgw charging transfer status

## Monitoring Data Path Measurements

---

Data path measurements include the following:

- Data path Gn statistics, including the number of incoming and outgoing GTP data packets and octets on the Gn interface
- Number of discarded GTP data packets
- Data path charging statistics, including per rating group (bearer) up and down packets and bytes
- Data path Gi or IP measurements, which does not include drops on the Gi Packet Forwarding Engine
- Incoming and outgoing packets and octets on the Gi interface
- Discarded packets
- Data path debug and miscellaneous statistics, which includes the number of sessions in progress, deleted sessions, source address violations, per APN access control list (ACL) violations, and so on.
- Per subscriber packet and byte statistics
- Per traffic class, per APN, and global packet and byte counts statistics
- IP measurements

### Related Documentation

- [Monitoring the Mobile Environment—Key Performance Indicators on page 3](#)
- [Monitoring Resources on page 4](#)

## Monitoring Call-Rate Statistics

---

The following metrics are available in real time to monitor the performance of the gateway call-rate indicators:

- Real-time measure of the 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

To monitor the call-rate statistics, execute the following command:

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

For more information, see the *show unified-edge ggsn-pgw call-rate statistics* topic in the *MobileNext Broadband Gateway Statements and Commands Reference Guide*.

**Related  
Documentation**

- [Monitoring the Mobile Environment—Key Performance Indicators on page 3](#)
- [Monitoring Data Rate Statistics on page 10](#)
- `show unified-edge ggsn-pgw call-rate statistics`

---

## Monitoring Data Rate Statistics

The data rate statistics can be monitored at the gateway level or at the APN level. Two sets of statistics can be monitored, one set for the Gn, Gp, S5, and S8 interfaces and one set for the Gi interface.

To monitor data rate statistics, do the following:

- To see the data plane statistics at the gateway level, execute the following command:

**user@host> show unified-edge ggsn-pgw statistics**

For more information, see the *show unified-edge ggsn-pgw statistics* topic in the *MobileNext Broadband Gateway Statements and Commands Reference Guide*.

- To see the data plane statistics at the APN level, execute the following command:

**user@host> show unified-edge ggsn-pgw apn statistics apn-name *apn-name***

For more information, see the *show unified-edge ggsn-pgw apn statistics* topic in the *MobileNext Broadband Gateway Statements and Commands Reference Guide*.

**Related  
Documentation**

- [Monitoring the Mobile Environment—Key Performance Indicators on page 3](#)
- [Monitoring Resources on page 4](#)
- `show unified-edge ggsn-pgw apn statistics`
- `show unified-edge ggsn-pgw statistics`

---

## Call Trace Overview

---

The MobileNext Broadband Gateway features many ways to monitor performance while the broadband gateways, either Gateway GPRS Support Nodes (GGSNs), Packet Data Network Gateways (P-GWs), or Serving Gateways (S-GWs), configured are in operational mode. In addition to the usual logging and alarm capabilities, the broadband gateways offer a call trace capability that allows operators with the required privileges to trace the progress of a call through the gateway in several ways, for example, by Mobile Station ISDN (MSISDN) or International Mobile Subscriber Identifier (IMSI).

You can initiate a call trace based on several criteria:

- Access Point Name (APN) (P-GW only)
- FPC slot
- PIC slot
- IMSI
- MSISDN
- Next call (up to fifty)

You can specify other information as well:

- Comment—A user-determined field used to help distinguish one call trace from another.
- File name prefix—A prefix for the call trace file name. This prefix is used with the user name and timestamp to determine the call trace file name.

You can perform several actions to manage the call trace monitor operation:

- Start the subscriber events trace
- Show the subscriber events trace information
- Stop the subscriber events trace
- Clear the subscriber events trace

Call trace offers another tool for broadband gateway performance monitoring and troubleshooting.

### Related Documentation

- [Monitoring the Mobile Environment—Key Performance Indicators on page 3](#)
- [Example: Monitoring a P-GW with Call Trace on page 12](#)
- [Example: Monitoring an S-GW with Call Trace on page 14](#)

## Example: Monitoring a P-GW with Call Trace

---

This example shows how to monitor MobileNext Broadband Gateway Packet Data Network Gateway (P-GW) operation with call trace.

- [Requirements on page 12](#)
- [Overview on page 12](#)
- [Configuration on page 12](#)

### Requirements

This example uses the following hardware and software components:

- An installed and operational MobileNext Broadband Gateway chassis
- The properly installed and Operational Junos OS MobileNext Broadband Gateway software packages

Before you use call trace for monitoring, be sure you have:

- Made sure that this P-GW is configured correctly

### Overview

This example shows how to monitor the P-GW operation using call trace.

#### Topology

---

This procedure is independent of other network devices.

### Configuration

To use call trace monitoring, perform these tasks:

- [Monitoring with Call Trace on page 12](#)

#### Monitoring with Call Trace

---

##### Step-by-Step Procedure

To use call trace monitoring:

1. Start the call trace with a file name prefix and comment.

```
user@MGB1> request unified-edge ggsn-pgw call-trace start imsi 101313783444554  
file-name-prefix mbgw1 comment friday trace
```



**NOTE:** This example uses IMSI number as the basis for the call trace.

Service PIC	Status
ms-0/0/0	success
ms-10/0/0	success

2. Display the call trace information.

```
user@MGB1> request unified-edge ggsn-pgw call-trace show detail
```

```
Identifier : call_trace_id_1    Trace file : call_trace_id_1_mbgw1_01142012_152946
Status : not-done Create Mask : 0x44 Complete Mask : 0x0
IMSI : 505002003476097
Calls Traced : 1
Comment: friday trace
```

3. Stop the call trace. You can stop all traces at once, as shown here.

```
user@MGB1> request unified-edge ggsn-pgw call-trace stop all
```

```
Service PIC Status
ms-0/0/0 success
ms-10/0/0 success
```

4. Display the available trace files.

```
user@MGB1> request unified-edge ggsn-pgw call-trace show
```

```
Identifier    File name          Status    SPIC Mask SPIC Mask
              create complete
call_trace_id_1 call_trace_id_1_mbgw1_01142012_152946 done 0x44 0x44

{master}
```

5. Display the contents of a call trace log file. Just as Syslog files, call traces are stored in `/var/log`.

```
user@MGB1> request unified-edge ggsn-pgw call-trace show
/var/log/call_trace_id_1_mbgw1_01142012_152946
```

```
Dec 5 16:12:30.1118022 cpu_id: [6] gtid: [9] tid: [2] app_id: 1 Encode: Encoding GTP
V1 Header
Dec 5 16:12:30.1118044 cpu_id: [6] gtid: [9] tid: [2] app_id: 1 Encode: Msg Type 17
SeqNumber 584 TEID 302149215
Dec 5 16:12:30.1118067 cpu_id: [6] gtid: [9] tid: [2] app_id: 1 Encode: Encoding
CAUSE IE
Dec 5 16:12:30.1118088 cpu_id: [6] gtid: [9] tid: [2] app_id: 1 Encode: Encoding cause
Authentication failure
Dec 5 16:12:30.1118109 cpu_id: [6] gtid: [9] tid: [2] app_id: 1 Encode: ERROR: Non
successful cause value(208) sent
Dec 5 16:12:30.1118131 cpu_id: [6] gtid: [9] tid: [2] app_id: 1 Encode: ENCODED Error
Response of length 14 for msg 17
```

```
Nov 26 16:20:53.1327494 cpu_id: [5] gtid: [8] tid: [1] app_id: 1 change reporting
action not supported
Nov 26 16:20:53.1327997 cpu_id: [5] gtid: [8] tid: [1] app_id: 1 Handler returned
PASS
Nov 26 16:20:53.1328020 cpu_id: [5] gtid: [8] tid: [1] app_id: 1 calling afProcessEvent
for event=sessUpdate, state=Established
Nov 26 16:20:53.1328042 cpu_id: [5] gtid: [8] tid: [1] app_id: 1 i = 0, size = 1,
evtProtocolBitmap = 19 info->cause = 0, info->sub_cause = 0
Nov 26 16:20:53.1328068 cpu_id: [5] gtid: [8] tid: [1] app_id: 1 calling session-evt
```

handler #0 for state=Established, event=sessUpdate info->cause = 0,  
info->subcause=0, num\_handlers=1

**Related  
Documentation**

- [Call Trace Overview on page 11](#)
- [Example: Monitoring an S-GW with Call Trace on page 14](#)
- [Monitoring the Mobile Environment—Key Performance Indicators on page 3](#)
- request unified-edge ggsn-pgw call-trace clear
- request unified-edge ggsn-pgw call-trace show
- request unified-edge ggsn-pgw call-trace start
- request unified-edge ggsn-pgw call-trace stop

---

## Example: Monitoring an S-GW with Call Trace

This example shows how to monitor MobileNext Broadband Gateway Serving Gateway (S-GW) operation with call trace.

- [Requirements on page 14](#)
- [Overview on page 14](#)
- [Configuration on page 14](#)

### Requirements

This example uses the following hardware and software components:

- An installed and operational MobileNext Broadband Gateway chassis
- The properly installed and Operational Junos OS MobileNext Broadband Gateway software packages

Before you use call trace for monitoring, be sure you have:

- Made sure that this S-GW is configured correctly

### Overview

This example shows how to monitor the S-GW operation using call trace.

---

#### Topology

This procedure is independent of other network devices.

### Configuration

To use call trace monitoring, perform these tasks:

- [Monitoring with Call Trace on page 15](#)



## Monitoring with Call Trace

### Step-by-Step Procedure

To use call trace monitoring:

1. Start the call trace with a file name prefix and comment..

```
user@MGB1> request unified-edge sgw call-trace start fpc-slot 4 pic-slot 0 next-call
10 file-name-prefix mbgw2 comment friday trace
```



**NOTE:** This example uses FPC and PIC and next-call option as the basis for the call trace.

```
Service PIC    Status
ms-0/0/0      success
ms-1/0/0      success
```

2. Display the call trace information.

```
user@MGB1> request unified-edge sgw call-trace show brief
```

```
Call trace information :
Identifier : call_trace_id_10  Trace file :
call_trace_id_10_mbgw2_02112012_205634
Status : done  Create Mask : 0x0  Complete Mask : 0x0
Next Call : 10
Calls Traced : 0    FPC : 5  PIC : 0
Identifier : call_trace_id_11  Trace file :
call_trace_id_11_mbgw2_02112012_205932
Status : done  Create Mask : 0x40  Complete Mask : 0x40
Calls Traced : 0
Identifier : call_trace_id_12  Trace file :
call_trace_id_12_mbgw2_02112012_210001
Status : not-done  Create Mask : 0x40  Complete Mask : 0x0
Next Call : 5
Calls Traced : 0    FPC : 4  PIC : 0
Identifier : call_trace_id_13  Trace file :
call_trace_id_13_mbgw2_02112012_210353
Status : duplicate  Create Mask : 0x0  Complete Mask : 0x0
Next Call : 5
Calls Traced : 0    FPC : 4  PIC : 0
Comment: friday trace
```

3. Stop the call trace. You can stop all traces at once, as shown here.

```
user@MGB1> request unified-edge sgw call-trace stop all
```

```
Service PIC    Status
ms-0/0/0      success
ms-1/0/0      success
```

4. Display the available trace files.

```
user@MGB1> request unified-edge sgw call-trace show
```

Identifier	File name	Status	SPIC Mask	SPIC Mask
		create	complete	
call_trace_id_1	call_trace_id_1_mbgw2_01142012_152946	done	0x44	0x44

{master}

5. Display the contents of a call trace log file. Just as Syslog files, call traces are stored in `/var/log`.

```
user@MGB1> request unified-edge sgw call-trace show  
/var/log/call_trace_id_1_mbgw2_01142012_152946
```

```
Dec 5 16:12:30.1118022 cpu_id: [6] gtid: [9] tid: [2] app_id: 1 Encode: Encoding GTP  
V1 Header  
Dec 5 16:12:30.1118044 cpu_id: [6] gtid: [9] tid: [2] app_id: 1 Encode: Msg Type 17  
SeqNumber 584 TEID 302149215  
Dec 5 16:12:30.1118067 cpu_id: [6] gtid: [9] tid: [2] app_id: 1 Encode: Encoding  
CAUSE IE  
Dec 5 16:12:30.1118088 cpu_id: [6] gtid: [9] tid: [2] app_id: 1 Encode: Encoding cause  
Authentication failure  
Dec 5 16:12:30.1118109 cpu_id: [6] gtid: [9] tid: [2] app_id: 1 Encode: ERROR: Non  
successful cause value(208) sent  
Dec 5 16:12:30.1118131 cpu_id: [6] gtid: [9] tid: [2] app_id: 1 Encode: ENCODED Error  
Response of length 14 for msg 17
```

```
Nov 26 16:20:53.1327494 cpu_id: [5] gtid: [8] tid: [1] app_id: 1 change reporting  
action not supported  
Nov 26 16:20:53.1327997 cpu_id: [5] gtid: [8] tid: [1] app_id: 1 Handler returned  
PASS  
Nov 26 16:20:53.1328020 cpu_id: [5] gtid: [8] tid: [1] app_id: 1 calling afProcessEvent  
for event=sessUpdate, state=Established  
Nov 26 16:20:53.1328042 cpu_id: [5] gtid: [8] tid: [1] app_id: 1 i = 0, size = 1,  
evtProtocolBitmap = 19 info->cause = 0, info->sub_cause = 0  
Nov 26 16:20:53.1328068 cpu_id: [5] gtid: [8] tid: [1] app_id: 1 calling session-evt  
handler #0 for state=Established, event=sessUpdate info->cause = 0,  
info->subcause=0, num_handlers=1
```

**Related  
Documentation**

- [Call Trace Overview on page 11](#)
- [Example: Monitoring a P-GW with Call Trace on page 12](#)
- [Monitoring the Mobile Environment—Key Performance Indicators on page 3](#)
- request unified-edge sgw call-trace clear
- request unified-edge sgw call-trace show
- request unified-edge sgw call-trace start
- request unified-edge sgw call-trace stop

## PART 2

# Troubleshooting

- [Troubleshooting on page 19](#)



## CHAPTER 2

# Troubleshooting

This chapter describes the proper actions to take to restore network health when performance or processes are not behaving as expected.

- [Troubleshooting Mobility Overview on page 19](#)
- [Request Support Information Overview on page 20](#)
- [Troubleshooting Overload Conditions in the Mobile Network on page 20](#)
- [Troubleshooting Multilevel Overload Protection on page 21](#)
- [Responding to an Overload on page 21](#)
- [Monitoring GTP Signaling on page 22](#)
- [Troubleshooting Call Admission Control on page 23](#)
- [Monitoring AAA Metrics on page 25](#)

### Troubleshooting Mobility Overview

This chapter describes the proper action to take to restore network health when performance or processes are not behaving as expected.

Modern networks, such as mobile networks, do not often fail to do anything at all. Modern networks don't really break: they get "sick." The network is still functioning, but parts of it are not doing what they are supposed to.

The root problem is sometimes difficult to isolate and fix. Troubleshooting does not work in isolation, but functions along with monitoring tools put in place since installation. These provide information about how the network should work, and not just when it fails. Unless you set up ways to monitor and operate your network in good times, you'll be hard pressed to zoom right to the trouble area in bad times.

Operations monitoring forms the baseline for troubleshooting. Otherwise, the network is visible only when it is malfunctioning. No network is too small to expend resources on keeping event tracking logs. There are some essential Junos OS tools for network monitoring, including system logging (syslog), SNMP polling, SNMP traps, and CLI show commands. The first three are generic to all Juniper Networks devices and are not repeated here. The basic mobility troubleshooting tool is the CLI show command for mobility components.

- Related Documentation**
- [Monitoring AAA Metrics on page 25](#)
  - [Monitoring GTP Signaling on page 4](#)
  - [Request Support Information Overview on page 20](#)
  - [Responding to an Overload on page 21](#)
  - [Troubleshooting Call Admission Control on page 23](#)
  - [Troubleshooting Multilevel Overload Protection on page 21](#)
  - [Troubleshooting Overload Conditions in the Mobile Network on page 20](#)

---

## Request Support Information Overview

You use the **request support information** command to gather information about the MobileNext Broadband Gateway before contacting customer support. You include this information in your support request. You save the result by piping the request through the **save** command.

Output from the **request support information** command varies depending on platform and installed software. The mobile version of the **request support information** command provides detailed information about the hardware and software configuration of the broadband gateway. The command always executes a series of **show** commands with the appropriate information for the broadband gateway automatically included.

The **request support information** command includes the configuration (except for secret data) and any core files.

- Related Documentation**
- [Monitoring AAA Metrics on page 25](#)
  - [Monitoring GTP Signaling on page 4](#)
  - [Responding to an Overload on page 21](#)
  - [Troubleshooting Call Admission Control on page 23](#)
  - [Troubleshooting Mobility Overview on page 19](#)
  - [Troubleshooting Multilevel Overload Protection on page 21](#)
  - [Troubleshooting Overload Conditions in the Mobile Network on page 20](#)

---

## 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**

- [Monitoring AAA Metrics on page 25](#)
- [Monitoring GTP Signaling on page 4](#)
- [Request Support Information Overview on page 20](#)
- [Responding to an Overload on page 21](#)
- [Troubleshooting Call Admission Control on page 23](#)
- [Troubleshooting Mobility Overview on page 19](#)
- [Troubleshooting Multilevel Overload Protection on page 21](#)

---

## 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**

- [Monitoring AAA Metrics on page 25](#)
- [Monitoring GTP Signaling on page 4](#)
- [Request Support Information Overview on page 20](#)
- [Responding to an Overload on page 21](#)
- [Troubleshooting Call Admission Control on page 23](#)
- [Troubleshooting Mobility Overview on page 19](#)
- [Troubleshooting Overload Conditions in the Mobile Network on page 20](#)

---

## 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**

- [Monitoring AAA Metrics on page 25](#)
- [Monitoring GTP Signaling on page 4](#)
- [Request Support Information Overview on page 20](#)
- [Troubleshooting Call Admission Control on page 23](#)
- [Troubleshooting Mobility Overview on page 19](#)
- [Troubleshooting Overload Conditions in the Mobile Network on page 20](#)
- [Troubleshooting Multilevel Overload Protection on page 21](#)

---

## 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 the following:

- Per peer history
- Per GTP cause code statistics for granular measurement of the number of failures
- Separate session establishments attempts and 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, execute the following command:

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

For more information, see the *show unified-edge ggsn-pgw resource-manager clients* topic in the *MobileNext Broadband Gateway Statements and Commands Reference Guide*.

2. To see a summary of subscribers on the gateway, execute the following command:

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

For more information, see the *show unified-edge ggsn-pgw status* topic in the *MobileNext Broadband Gateway Statements and Commands Reference Guide*.

3. To see subscriber details, execute the following command:

```
user@host> show unified-edge ggsn-pgw subscribers extensive
```



For more information, see the *show unified-edge ggsn-pgw subscribers* topic in the *MobileNext Broadband Gateway Statements and Commands Reference Guide*.

4. To see all GTP statistics (including messages sent and received, and cause codes sent and received), execute the following command:

```
user@host> show unified-edge ggsn-pgw gtp statistics detail
```

For more information, see the *show unified-edge ggsn-pgw gtp statistics* topic in the *MobileNext Broadband Gateway Statements and Commands Reference Guide*.

5. To see all the GTP peers, execute the following command:

```
user@host> show unified-edge ggsn-pgw gtp peer detail
```

For more information, see the *show unified-edge ggsn-pgw gtp peer* topic in the *MobileNext Broadband Gateway Statements and Commands Reference Guide*.

#### Related Documentation

- [Monitoring AAA Metrics on page 25](#)
- [Monitoring the Mobile Environment—Key Performance Indicators on page 3](#)
- [Monitoring Resources on page 4](#)
- [Request Support Information Overview on page 20](#)
- [Responding to an Overload on page 21](#)
- `show unified-edge ggsn-pgw gtp peer`
- `show unified-edge ggsn-pgw gtp statistics`
- `show unified-edge ggsn-pgw resource-manager clients`
- `show unified-edge ggsn-pgw status`
- `show unified-edge ggsn-pgw subscribers`
- [Troubleshooting Call Admission Control on page 23](#)
- [Troubleshooting Mobility Overview on page 19](#)
- [Troubleshooting Multilevel Overload Protection on page 21](#)
- [Troubleshooting Overload Conditions in the Mobile Network on page 20](#)

## Troubleshooting Call 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 profiles configured on your system. A classifier profile 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 profiles on your system. Therefore, understanding how these multiple classifier profiles 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.
- Maximum bearers configuration for the gateway
- High or low threshold percentages for CPU, memory, 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 more information, see the *show unified-edge ggsn-pgw subscribers* topic in the *MobileNext Broadband Gateway Statements and Commands Reference Guide*.

- For preemption lists (priority levels), use the command:

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

For more information, see the *show unified-edge ggsn-pgw status preemption-list* topic in the *MobileNext Broadband Gateway Statements and Commands Reference Guide*.

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 executing the following command:

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

For more information, see the *show unified-edge ggsn-pgw call-admission-control statistics* topic in the *MobileNext Broadband Gateway Statements and Commands Reference Guide*.

**Related Documentation**

- [Monitoring AAA Metrics on page 25](#)
- [Monitoring GTP Signaling on page 4](#)
- [Request Support Information Overview on page 20](#)
- [Responding to an Overload on page 21](#)
- [Troubleshooting Mobility Overview on page 19](#)
- [Troubleshooting Multilevel Overload Protection on page 21](#)
- [Troubleshooting Overload Conditions in the Mobile Network on page 20](#)
- `show unified-edge ggsn-pgw call-admission-control statistics`
- `show unified-edge ggsn-pgw status preemption-list`
- `show unified-edge ggsn-pgw subscribers`

## 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`

**Related  
Documentation**

- [Monitoring GTP Signaling on page 4](#)
- [Request Support Information Overview on page 20](#)
- [Responding to an Overload on page 21](#)
- [Troubleshooting Call Admission Control on page 23](#)
- [Troubleshooting Mobility Overview on page 19](#)
- [Troubleshooting Multilevel Overload Protection on page 21](#)
- [Troubleshooting Overload Conditions in the Mobile Network on page 20](#)





## PART 3

# Index

- [Index on page 33](#)



# Index

## Symbols

#, comments in configuration statements.....	viii
( ), in syntax descriptions.....	viii
< >, in syntax descriptions.....	vii
[ ], in configuration statements.....	viii
{ }, in configuration statements.....	viii
(pipe), in syntax descriptions.....	viii

## A

AAA troubleshooting.....	25
--------------------------	----

## B

braces, in configuration statements.....	viii
brackets	
angle, in syntax descriptions.....	vii
square, in configuration statements.....	viii
broadband gateway	
support information.....	20

## C

call admission control	
troubleshooting.....	23
call trace	
overview.....	11
P-GW example.....	12
S-GW example.....	14
call-rate statistics	
monitoring.....	9
charging gateways	
monitoring.....	7
comments, in configuration statements.....	viii
conventions	
text and syntax.....	vii
CPU indicators	
monitoring.....	6
curly braces, in configuration statements.....	viii
customer support.....	viii
contacting JTAC.....	viii

## D

data path measurements	
monitoring.....	9
data rate statistics	
monitoring.....	10
documentation	
comments on.....	viii

## E

example	
monitoring P-GW with call trace.....	12
monitoring S-GW with call trace.....	14

## F

font conventions.....	vii
-----------------------	-----

## G

GTP signaling	
monitoring.....	4, 22

## I

icons defined, notice.....	vi
----------------------------	----

## K

key performance indicators	
monitoring.....	3

## M

manuals	
comments on.....	viii
memory indicators	
monitoring.....	7
mobile environment	
monitoring.....	3
mobility	
troubleshooting.....	19
monitoring	
call trace example.....	12, 14
multilevel overload protection	
troubleshooting.....	21

## N

notice icons defined.....	vi
---------------------------	----

## O

overload	
responding.....	21
overload conditions	
troubleshooting.....	20

overview	
call trace.....	11
<b>P</b>	
P-GW	
call trace example.....	12
parentheses, in syntax descriptions.....	viii
<b>R</b>	
resources	
monitoring.....	4
<b>S</b>	
S-GW	
call trace example.....	14
session status	
monitoring.....	6
support information	
on broadband gateway.....	20
support, technical See technical support	
syntax conventions.....	vii
<b>T</b>	
technical support	
contacting JTAC.....	viii
troubleshooting mobility.....	19