



Monitoring Notifications

This appendix describes enabling and monitoring Gateway GPRS Support Node (GGSN) SNMP notifications to manage GPRS/UMTS-related issues. SNMP uses notifications to report events on a managed device. The notifications are traps or informs for different events.



Note

This appendix covers enabling and monitoring GGSN SNMP notifications only. Additional types of SNMP notifications can be enabled on your Cisco router. For more information about the types of SNMP notifications you can enable, see the *Cisco IOS Configuration Fundamentals*, Release 12.3 documentation.

Additionally, to display a list of notifications available on your Cisco router, enter the **snmp-server enable traps ?** command.

This appendix contains the following sections:

- [SNMP Overview, page A-33](#)
- [Configuring MIB Support, page A-38](#)
- [Enabling SNMP Support, page A-41](#)
- [Enabling and Disabling GGSN SNMP Notifications, page A-41](#)
- [GGSN SNMP Notifications, page A-42](#)

SNMP Overview

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a standardized framework and a common language used for monitoring and managing devices in a network.

The SNMP framework has three parts:

- **SNMP manager**—A system used to control and monitor the activities of network hosts using SNMP. The most common managing system is called a Network Management System (NMS). The term NMS can be applied to either a dedicated device used for network management, or the applications used on a network-management device. A variety of network management applications are available for use with SNMP. These features range from simple command-line applications to feature-rich graphical user interfaces (such as the CiscoWorks2000 line of products).

- **SNMP agent**—A software component in a managed device that maintains the data for the device and reports the data, as needed, to managing systems. The agent and MIB reside on the routing device (router, access server, or switch). To enable the SNMP agent on a managed device, you must define the relationship between the manager and the agent (see the [“Enabling SNMP Support” section on page A-41](#)).
- **Management Information Base (MIB)**—Collection of network-management information, organized hierarchically.

Instead of defining a large set of commands, SNMP places all operations in a get-request, get-next-request, and set-request format. For example, an SNMP manager can get a value from an SNMP agent or set a value in that SNMP agent.

MIB Description

A Management Information Base (MIB) is a collection of network-management information, organized hierarchically. The MIB consists of collections of managed objects identified by object identifiers. MIBs are accessed using a network-management protocol such as SNMP. A managed object (sometimes called a MIB object or an object) is one of a number of characteristics of a managed device, such as a router. Managed objects comprise one or more object instances, which are essentially variables. The Cisco implementation of SNMP uses the definitions of MIB II variables described in RFC 1213.

MIBs can contain two types of managed objects:

- **Scalar objects**—Define a single object instance (for example, `ifNumber` in the IF-MIB and `bgpVersion` in the BGP4-MIB).
- **Columnar objects**—Defines a MIB table that contains no rows or more than one row, and each row can contain one or more scalar objects, (for example, `ifTable` in the IF-MIB defines the interface).

System MIB variables are accessible through SNMP as follows:

- **Accessing a MIB variable**—Function is initiated by the SNMP agent in response to a request from the NMS. The agent retrieves the value of the requested MIB variable and responds to the NMS with that value.
- **Setting a MIB variable**—Function is initiated by the SNMP agent in response to a message from the NMS. The SNMP agent changes the value of the MIB variable to the value requested by the NMS.

SNMP Notifications

An SNMP agent can notify the manager when important system events occur, such as the following:

- An interface or card starts or stops running
- Temperature thresholds are crossed
- Authentication failures occur

When an agent detects an alarm condition, the agent:

- Logs information about the time, type, and severity of the condition
- Generates a notification message, which it then sends to a designated IP host

SNMP notifications are sent as either:

- Traps—Unreliable messages, which do not require receipt acknowledgment from the SNMP manager.
- Informs—Reliable messages, which are stored in memory until the SNMP manager issues a response. Informs use more system resources than traps.



Note Many commands use the word traps in the command syntax. Unless there is an option in the command to select either traps or informs, the keyword traps refers to either traps, informs, or both. Use the **snmp-server host** command to specify whether to send SNMP notifications as traps or informs.

When an agent detects an alarm condition, it logs information about the time, type, and severity of the condition and generates a notification message, which it then sends to a designated IP host.

SNMP notifications can be sent as either *traps* or *informs*. See the [“Enabling SNMP Support” section on page A-41](#) for instructions on how to enable traps on the GGSN. See the [“GGSN SNMP Notifications” section on page A-42](#) for information about GGSN traps.

The Cisco implementation of SNMP uses the definitions of SNMP traps described in RFC 1215.

SNMP Versions

Cisco IOS software supports the following versions of SNMP:

- SNMPv1—The Simple Network Management Protocol: An Internet standard, defined in RFC 1157. Security is based on community strings.
- SNMPv2c—The community-string based administrative framework for SNMPv2. SNMPv2c is an update of the protocol operations and data types of SNMPv2p (SNMPv2 classic), and uses the community-based security model of SNMPv1.
- SNMPv3—Version 3 of SNMP. SNMPv3 uses the following security features to provide secure access to devices:
 - Message integrity—Ensuring that a packet has not been tampered with in transit.
 - Authentication—Determining that the message is from a valid source.
 - Encryption—Scrambling the contents of a packet to prevent it from being learned by an unauthorized source.

SNMPv1 and SNMPv2c

Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers who are able to access the agent MIB is defined by an IP address Access Control List and password.

SNMPv2c support includes a bulk-retrieval mechanism and more detailed error message reporting to management stations. The bulk-retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round-trip transmissions required. SNMPv2c improved error handling support includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes now report the error type. Three kinds of exceptions are also reported:

- no such object exceptions
- no such instance exceptions
- end of MIB view exceptions

SNMPv3

SNMPv3 provides the following security models and security levels:

- Security model—Authentication strategy that is set up for a user and the group in which the user resides.
- Security level—Permitted level of security within a security model.

A combination of a security model and a security level determines the security mechanism to be employed when handling an SNMP packet.

SNMP Security Models and Levels

Table 0-1 describes the security models and levels provided by the different SNMP versions.

Table 0-1 *SNMP Security Models and Levels*

| Model | Level | Authentication | Encryption | Description |
|-------|--------------|------------------|------------|--|
| v1 | noAuthNoPriv | Community string | No | Uses match on community string for authentication. |
| v2c | noAuthNoPriv | Community string | No | Uses match on community string for authentication. |
| v3 | noAuthNoPriv | User name | No | Uses match on user name for authentication. |
| v3 | authNoPriv | MD5 or SHA | No | Provides authentication based on HMAC-MD5 or HMAC-SHA algorithm. |
| v3 | authPriv | MD5 or SHA | DES | Provides authentication based on HMAC-MD5 or HMAC-SHA algorithm. Also provides DES 56-bit encryption based on CBC-DES (DES-56) standard. |

You must configure the SNMP agent to use the version of SNMP supported by the management station. An agent can communicate with multiple managers; for this reason, you can configure the Cisco IOS software to support communications with one management station using the SNMPv1 protocol, one using the SNMPv2c protocol, and another using SMNPv3.

Requests for Comments

MIB modules are written in the SNMP MIB module language, and are typically defined in Request For Comments (RFC) documents submitted to the Internet Engineering Task Force (IETF). RFCs are written by individuals or groups for consideration by the Internet Society and the Internet community as a whole. Before being given RFC status, recommendations are published as Internet Draft (I-D) documents. RFCs that have become recommended standards are also labeled as standards (STD) documents. For more information, see the Internet Society and IETF websites (<http://www.isoc.org> and <http://www.ietf.org>).

We provide private MIB extensions with each Cisco system. Cisco enterprise MIBs comply with the guidelines described in the relevant RFCs unless otherwise noted in the documentation.

Object Identifiers

An object identifier (OID) uniquely identifies a MIB object on a managed network device. The OID identifies the MIB object's location in the MIB hierarchy, and provides a means of accessing the MIB object in a network of managed devices:

- Standard RFC MIB OIDs are assigned by the Internet Assigned Numbers Authority (IANA)
- Enterprise MIB OIDs are assigned by Cisco Assigned Numbers Authority (CANA).

Each number in the OID corresponds to a level of MIB hierarchy. For example, the OID 1.3.6.1.4.1.9.9.xyz represents the xyz-MIB whose location in the MIB hierarchy is as follows. Note that the numbers in parentheses are included only to help show correspondence to the MIB hierarchy. In actual use, OIDs are represented as numerical values only.

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).cisco(9).ciscoMgt(9).nn-MIB

You can uniquely identify a managed object, such as ifNumber in the IF-MIB, by its object name (iso.org.dod.internet.mgmt.enterprises.interfaces.ifNumber) or by its OID (1.3.6.1.2.1.2.1).

For a list of OIDs assigned to MIB objects, go to the following URL:

<ftp://ftp.cisco.com/pub/mibs/oid/>

Related Information and Useful Links

The following URL provides access to general information about Cisco MIBs. Use the links on this page to access MIBs for download, and to access related information (such as application notes and OID listings).

- <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

TAC Information and FAQs

The following URLs provide access to SNMP information developed by the Cisco Technical Assistance Center (TAC):

- <http://www.cisco.com/warp/public/477/SNMP/index.html> is the Cisco TAC page for SNMP. It provides links to general SNMP information and tips for using SNMP to gather data.
- http://www.cisco.com/warp/public/477/SNMP/mibs_9226.shtml is a list of frequently asked questions (FAQs) about Cisco MIBs.

SNMP Configuration Information

The following URLs provide information about configuring SNMP:

- http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun_c/fcprt3/fcmonitr.htm provides general information about configuring SNMP support. It is part of the *Cisco IOS Configuration Fundamentals Configuration Guide*.
- http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/fun_r/frprt3/frmonitr.htm provides information about SNMP commands. It is part of the *Cisco IOS Configuration Fundamentals Command Reference*.

Configuring MIB Support

This chapter describes how to configure SNMP and MIB support on a Cisco router. It includes the following sections:

- [Determining MIBs Included for Cisco IOS Releases, page A-38](#)
- [Downloading and Compiling MIBs, page A-39](#)
- [Enabling SNMP Support, page A-41](#)

Determining MIBs Included for Cisco IOS Releases

Follow these steps to determine which MIBs are included in the Cisco IOS release you are using:

-
- Step 1** Go to the Feature Navigator home page <http://tools.cisco.com/ITDIT/MIBS/servlet/index>.
- Step 2** Click **MIB Locator** to launch the application. The MIB Locator application allows you to find a MIB in the following three ways:
- a. By release, platform family, and feature set—From the MIB Locator page:
 - Click the drop-down menu and select the desired Cisco IOS software release.
 - From the Platform Family menu, select 7600-MWAM/Cat6000-MWAM or 7200 (depending on which platform you are using). If you select the platform first, the system displays only those releases and feature sets that apply to the platform you have selected.
 - From the Feature Set menu, select the appropriate GGSN release.

- b. By image name—From the MIB Locator page, enter the GGSN image name you are using into the Search by Image Name field and click **Submit**: (the following image name is an example):

```
c6svcmwam-g8is-mz.123-14.YQ.bin
```

- c. By MIB name—From the MIB Locator page, search for the MIB from the list of MIBs in the Search for a MIB menu. You can select one, or for a multiple selection, hold down the **CTRL** key, then click **Submit**.



Note After you make a selection, follow the links and instructions.

Downloading and Compiling MIBs

The following sections provide information about how to download and compile MIBs for the GGSN:

- [Considerations for Working with MIBs](#)
- [Downloading MIBs](#)
- [Compiling MIBs](#)

Considerations for Working with MIBs

While working with MIBs, consider the following:

Mismatches on Datatype Definitions

- Mismatches on datatype definitions might cause compiler errors or warning messages. Although Cisco MIB datatype definitions are not mismatched, standard RFC MIBs do mismatch. For example:

```
MIB A defines: SomeDatatype ::= INTEGER(0..100)
MIB B defines: SomeDatatype ::= INTEGER(1..50)
```

This example is considered to be a trivial error and the MIB loads successfully with a warning message.

The next example is considered a nontrivial error (even though the two definitions are essentially equivalent), and the MIB is not successfully parsed.

```
MIB A defines: SomeDatatype ::= DisplayString
MIB B defines: SomeDatatype ::= OCTET STRING (SIZE(0..255))
```

If your MIB compiler treats these as errors, or you want to delete the warning messages, edit one of the MIBs that define this same datatype so that the definitions match.

- Many MIBs import definitions from other MIBs. If your management application requires MIBs to be loaded, and you experience problems with undefined objects, you might want to load the following MIBs in this order:

```
SNMPv2-SMI.my
SNMPv2-TC.my
SNMPv2-MIB.my
RFC1213-MIB.my
IF-MIB.my
```

CISCO-SMI.my
 CISCO-PRODUCTS-MIB.my
 CISCO-TC.my

- For additional information and SNMP technical tips, from the Locator page, click **SNMP MIB Technical Tips** and follow the links or go to the following URL:
http://www.cisco.com/cgi-bin/Support/browse/psp_view.pl?p=Internetworking:SNMP&s=Implementation_and_Configuration#Samples_and_Tips
- For a list of SNMP object identifiers (OIDs) assigned to MIB objects, go to the following URL and click on **SNMP Object Navigator** and follow the links:
<http://tools.cisco.com/ITDIT/MIBS/servlet/index>



Note You must have a Cisco CCO name and password to access the MIB Locator.

- For information about how to download and compile Cisco MIBs, go to the following URL:
<http://www.cisco.com/warp/public/477/SNMP/mibcompilers.html>

Downloading MIBs

Follow these steps to download the MIBs onto your system if they are not already there:

-
- Step 1** Review the considerations in the previous section (“[Considerations for Working with MIBs](#)”).
- Step 2** Go to one of the following Cisco URLs. If the MIB you want to download is not there, try the other URL; otherwise, go to one of the URLs in Step 5.
- <ftp://ftp.cisco.com/pub/mibs/v2>
<ftp://ftp.cisco.com/pub/mibs/v1>
- Step 3** Click the link for a MIB to download that MIB to your system.
- Step 4** Select **File > Save** or **File > Save As** to save the MIB on your system.
- Step 5** You can download industry-standard MIBs from the following URLs:
- <http://www.ietf.org>
 - <http://www.atmforum.com>
-

Compiling MIBs

If you plan to integrate the Cisco router with an SNMP-based management application, then you must also compile the MIBs for that platform. For example, if you are running HP OpenView on a UNIX operating system, you must compile platform MIBs with the HP OpenView Network Management System (NMS). For instructions, see the NMS documentation.

Enabling SNMP Support

The following procedure summarizes how to configure the Cisco router for SNMP support.

For detailed information about SNMP commands, see the following Cisco documents:

- *Cisco IOS Release 12.3 Configuration Fundamentals Configuration Guide*, “Monitoring the Router and Network” section, available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/index.htm

- *Cisco IOS Release 12.3 Configuration Fundamentals Command Reference*, Part 3: System Management Commands, “Router and Network Configuration Commands” section, available at the the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_r/index.htm

To configure the Cisco router for SNMP support, follow these steps:

Step 1 Set up your basic SNMP configuration through the command line interface (CLI) on the router. Note that these basic configuration commands are issued for SNMPv2c. For SNMPv3, you must also set up SNMP users and groups. (See the preceding list of documents for command and setup information.)

- a. Define SNMP read-only and read-write communities:

```
Router (config)# snmp-server community Read_Only_Community_Name ro
Router (config)# snmp-server community Read_Write_Community_Name rw
```

- b. Configure SNMP views (to limit the range of objects accessible to different SNMP user groups):

```
Router (config)# snmp-server view view_name oid-tree {included | excluded}
```

Enabling and Disabling GGSN SNMP Notifications

To use the command line interface (CLI) to enable the Cisco router to send GGSN SNMP notifications (traps or informs), perform the following steps.

Step 1 Make sure SNMP is configured on the router (see the “[Enabling SNMP Support](#)” section on page A-41).

Step 2 Identify (by IP address) the host to receive traps from the Cisco router:

```
Router(config)#snmp-server host host-address version SNMP version community/user(V3)
udp-port <UDP port No>
```

Step 3 Enable GGSN SNMP notifications on the Cisco router using the following command (enter a separate command for each type of notification you want to enable):

```
Router(config)#snmp-server enable traps gprs [apn | charging | ggsn | ggsn-apn |
ggsn-general | ggsn-memory | ggsn-pdp | ggsn-service | gtp]
```

Where:

- **apn**—Enables APN notifications.
- **charging**—Enables charging notifications.
- **ggsn**—Enables GGSN global notifications.



Note To prevent flooding, configuring the **snmp-server enable traps gprs ggsn** command enables all GGSN-related traps except for the `cGgsnGlobalErrorNotif`, `cGgsnAccessPointNameNotif`, and the `cGgsnPacketDataProtocolNotif` traps.

- **ggsn-apn**—Enables GGSN notifications specific to APN (`cGgsnAccessPointNameNotif`).
- **ggsn-general**—Enables GGSN general notifications (`cGgsnGlobalErrorNotif`).
- **ggsn-pdp**—Enables GGSN notifications specific to PDP (`cGgsnPacketDataProtocolNotif`).
- **ggsn-service**—Enables GGSN service-mode notifications.
- **gtp**—Enables GTP traps.



Note Issuing the **snmp-server enable traps gprs** command without a keyword option enables all GGSN SNMP notifications.

Step 4 To disable GGSN SNMP notifications on the Cisco router, enter the following command.

```
Router(config)# no snmp-server enable traps gprs
```

If you omit the notification type keyword (**gprs** in this example), all notifications are disabled.



Note We recommend that the **snmp-server enable traps gtp** command not be configured because all associated MIBs are deprecated.

GGSN SNMP Notifications

This section lists and briefly describes the notifications supported by GGSN MIBs and generated by the GGSN.

This section lists the following types of notifications:

- [Global Notifications, page A-43](#)
- [Charging Traps, page A-45](#)
- [Access-Point Notifications, page A-46](#)
- [Alarm Notifications, page A-47](#)

Global Notifications

Table A-2 lists the global notifications supported by the CISCO-GGSN-MIB. To enable these notifications to be sent, use the **snmp-server enable traps grps** global configuration command, with the **ggsn**, **ggsn-apn**, **ggsn-memory**, **ggsn-pdp**, and/or **ggsn-service** keyword option specified.



Note Issue a separate command for each keyword option.



Note cGgsnNotification (1.2.6.1.4.1.9.9.240.2.0.1) has been deprecated.

Table A-2 Global Notifications

| Notification and Notification Objects | Notes |
|--|--|
| cGgsnInServiceNotif (1.3.6.1.4.1.9.9.240.2.0.2) | <p>Sent when the GGSN is placed in operational (inService) mode.</p> <p>The GGSN is placed in operational mode using the grps service-mode operational global configuration command or by setting the cGgsnServiceMode object to inService(1).</p> <p>The service mode is identified by cGgsnServiceModeStatus.</p> <p>Enable the generation of this notification by setting cGgsnServiceNotifEnabled to true(1).</p> |
| cGgsnMaintenanceNotif (1.3.6.1.4.1.9.9.240.2.0.3) | <p>Sent when the GGSN is placed in maintenance mode.</p> <p>The GGSN is placed in maintenance mode using the grps service-mode maintenance global configuration command or by setting the cGgsnServiceMode object to maintenance(2).</p> <p>The service mode is identified by cGgsnServiceModeStatus.</p> <p>Enable the generation of this notification by setting cGgsnServiceNotifEnabled to true(1).</p> |
| cGgsnMemThresholdReachedNotif (1.3.6.1.4.1.9.9.240.2.0.4) | <p>Sent when the GGSN memory threshold has been reached.</p> <p>The memory threshold is set using the grps memory threshold global configuration command or by setting cGgsnMemoryThreshold.</p> <p>Enable the generation of this notification by setting cGgsnMemoryNotifEnabled to true(1).</p> |
| cGgsnMemThresholdClearedNotif (1.3.6.1.4.1.9.9.240.2.0.5) | <p>Sent when the GGSN retains the memory and falls below the configured threshold.</p> <p>The memory threshold is set using the grps memory threshold global configuration command or by setting cGgsnMemoryThreshold.</p> <p>Enable the generation of this notification by setting cGgsnMemoryNotifEnabled to true(1).</p> |

Table A-2 Global Notifications (continued)

| Notification and Notification Objects | Notes |
|---|--|
| <p>cGgsnGlobalErrorNotif (1.3.6.1.4.1.9.9.240.2.0.8)</p> <p>cGgsnGlobalErrorTypes cGgsnHistNotifSeverity cGgsnHistNotifTimestamp cGgsnHistNotifGgsnIpAddrType cGgsnHistNotifGgsnIpAddr cGgsnHistNotifInfo</p> | <p>Sent when a GGSN-related alarm has occurred.</p> <p>If additional information is available for specific types of alarms, that information might be appended to the end of the notification in additional varbinds.</p> <p>Enable the generation of this notification by setting the cGgsnGlobalErrorNotifEnabled to true(1).</p> <p>Note To prevent flooding, cGgsnGlobalErrorNotif, cGgsnAccessPointNameNotif, and cGgsnPacketDataProtocolNotif replace cGgsnNotification in GGSN Release 5.1 and later.</p> <p>For information about cGgsnGlobalErrorNotif alarms, see the “cGgsnGlobalErrorNotif” section on page A-48.</p> |
| <p>cGgsnAccessPointNameNotif (1.3.6.1.4.1.9.9.240.2.0.9)</p> <p>cGgsnAccessPointErrorTypes cGgsnHistNotifSeverity cGgsnHistNotifTimestamp cGgsnHistNotifGgsnIpAddrType cGgsnHistNotifGgsnIpAddr cGgsnHistNotifInfo cGgsnNotifAccessPointName</p> | <p>Sent when an APN-related alarm has occurred.</p> <p>If additional information is available for specific types of alarms, that information might be appended to the end of the notification in additional varbinds.</p> <p>Enable the generation of this notification by setting the cGgsnAccessPointNotifEnabled to true(1).</p> <p>Note To prevent flooding, cGgsnGlobalErrorNotif, cGgsnAccessPointNameNotif, and cGgsnPacketDataProtocolNotif replace cGgsnNotification in GGSN Release 5.1 and later.</p> <p>For information about cGgsnAccessPointNameNotif alarms, see the “cGgsnAccessPointNameNotif” section on page A-50.</p> |
| <p>cGgsnPacketDataProtocolNotif (1.3.6.1.4.1.9.9.240.2.0.10)</p> <p>cGgsnPacketDataProtoErrorTypes cGgsnHistNotifSeverity cGgsnHistNotifTimestamp cGgsnHistNotifGgsnIpAddrType cGgsnHistNotifGgsnIpAddr cGgsnHistNotifInfo cGgsnNotifPdpImsi</p> | <p>Sent when a user-related alarm has occurred.</p> <p>If additional information is available for specific types of alarms, that information might be appended to the end of the notification in additional varbinds.</p> <p>Enable the generation of this notification by setting the cGgsnPdpNotifEnabled to true(1).</p> <p>Note To prevent flooding, cGgsnGlobalErrorNotif, cGgsnAccessPointNameNotif, and cGgsnPacketDataProtocolNotif replace cGgsnNotification in GGSN Release 5.1 and later.</p> <p>For information about cGgsnPacketDataProtocolNotif alarms, see the “cGgsnPacketDataProtocolNotif” section on page A-52.</p> |

Charging Traps

Table A-3 lists the charging-related traps supported in the CISCO-GPRS-CHARGING-MIB. To enable these notifications to be sent, use the **snmp-server enable traps gprs charging** global configuration command.

Table A-3 Charging Notifications

| Notification and Notification Objects | Notes |
|---|--|
| cgprsCgAlarmNotif (1.3.6.1.4.1.9.9.192.2.0.1) cgprsCgAlarmHistType cgprsCgAlarmHistAddrType cgprsCgAlarmHistAddress cgprsCgAlarmHistSeverity cgprsCgAlarmHistInfo | <p>Sent when a charging-related alarm is detected in the managed system.</p> <p>This alarm is sent after an entry has been added to the cgprsCgAlarmHistTable.</p> <p>Enable the generation of this notification by setting the cgprsCgAlarmEnable to true(1).</p> <p>For information about cgprsCgAlarmNotif alarms, see the “CgprsCgAlarmNotif” section on page A-53.</p> |
| cgprsCgGatewaySwitchoverNotif (1.3.6.1.4.1.9.9.192.2.0.2) cgprsCgActiveChgGatewayAddrType cgprsCgActiveChgGatewayAddress cgprsCgOldChgGatewayAddress | <p>Sent when the active charging gateway has switched.</p> <p>The switchover to a new charging gateway occurs according to the value specified for the charging gateway switch timer. The charging gateway switch timer can be set using the</p> <p>The charging gateway switch timer can be set using the gprs charging server-switch-timer global configuration command or by setting cgprsCgGroupSwitchOverTime. The priority in which a new charging gateway is selected can be configured using the gprs charging switchover priority global configuration command or by setting cgprsCgSwitchOverPriority.</p> <p>Enable the generation of this notification by setting cgprsCGAlarmEnable to true(1).</p> |
| cgprsCgInServiceModeNotif (1.3.6.1.4.1.9.9.192.2.0.3) | <p>Sent when the GGSN charging function is placed in operational mode.</p> <p>The charging function of the GGSN is placed in operational mode using the gprs charging service-mode global configuration command or by setting the cgprsCgServiceMode object to operational(1).</p> <p>Enable the generation of this notification by setting cgprsCGAlarmEnable to true(1).</p> |
| cgprsCgMaintenanceModeNotif (1.3.6.1.4.1.9.9.192.2.0.4) | <p>Sent when the GGSN charging function is placed in maintenance mode.</p> <p>The charging function of the GGSN is placed in maintenance mode using the gprs charging service-mode global configuration command or by setting the cgprsCgServiceMode object to maintenance(2).</p> <p>Enable the generation of this notification by setting cgprsCGAlarmEnable to true(1).</p> |

Access-Point Notifications

Table A-4 lists access-point-related notifications supported by the CISCO-GPRS-ACC-PT-MIB. To enable these notifications to be sent, use the **snmp-server enable traps gprs apn** global configuration command.

Table A-4 Access-point Notifications

| Notification and Notification Objects | Notes |
|---|---|
| cgprsAccPtCfgNotif (1.3.6.1.4.1.9.9.183.2.0.1) cgprsAccPtCfgNotifAccPtIndex cgprsAccPtCfgNotifReason | <p>Sent when an access-point configuration has occurred.</p> <p>This notification is sent after an entry has been added to the cgprsAccPtCfgNotifHistTable.</p> <p>Enable the generation of this notification by setting the cgprsAccPtCfgNotifEnable to true(1).</p> <p>For information about cgprsAccPtCfgNotif alarms, see the “cgprsAccPtCfgNotif” section on page A-55.</p> |
| cgprsAccPtSecSrcViolNotif (1.3.6.1.4.1.9.9.183.2.0.2) cgprsAccPtCfgNotifAccPtIndex cgprsAccPtMsAddrType cgprsAccPtMsAllocAddr cgprsAccPtMsNewAddr | <p>Sent when a security violation has occurred, specifically, the GGSN determines that the source address of an upstream TPDU differs from that previously assigned to the MS.</p> <p>Enable the generation of this notification using the security verify source access-point configuration command or by setting the cgprsAccPtVerifyUpStrTpduSrcAddr object to true(1).</p> |
| cgprsAccPtSecDestViolNotif (1.3.6.1.4.1.9.9.183.2.0.3) cgprsAccPtCfgNotifAccPtIndex cgprsAccPtMsAddrType cgprsAccPtMsAllocAddr cgprsAccPtMsTpduDstAddr | <p>Sent when a security violation has occurred, specifically, the GGSN determines that the destination address of an upstream TPDU falls within the range of a user-defined global list of PLMN addresses.</p> <p>Enable the generation of this notification using the security verify destination access-point configuration command or by setting the cgprsAccPtVerifyUpStrTpduDstAddr object to true(1).</p> |
| cgprsAccPtMaintenanceNotif (1.3.6.1.4.1.9.9.183.2.0.4) cgprsAccPtCfgNotifAccPtIndex | <p>Sent when the APN is placed in maintenance mode.</p> <p>An APN is placed in maintenance mode using the service-mode maintenance access-point configuration command or by setting the cgprsAccPtOperationMode object to maintenance(1).</p> <p>The service mode is identified by cGgsnServiceModeStatus.</p> <p>Enable the generation of this notification by setting cgprsAccPtMaintenanceNotif to true(1).</p> |
| cgprsAccPtInServiceNotif (1.3.6.1.4.1.9.9.183.2.0.5) cgprsAccPtCfgNotifAccPtIndex | <p>Sent when the APN is placed in operational mode.</p> <p>An APN is placed in operational mode using the service-mode operational access-point configuration command or by setting cgprsAccPtOperationMode to inService(0).</p> <p>The service mode is identified by cGgsnServiceModeStatus.</p> <p>Enable the generation of this notification by setting cgprsAccPtMaintenanceNotif to true(1).</p> |

GTP Notification

Table A-4 lists the GTP-related notification supported by the CISCO-GTP-MIB. To enable this notification to be sent, use the **snmp-server enable traps gprs gtp** global configuration command.

Table A-5 *GTP Notification*

| Notification and Notification Objects | Notes |
|--|--|
| cGtpPathFailedNotification (1.3.6.1.4.1.9.9.188.2.0.1) cGtpLastNoRespToEchoGSNIpAddrTyp cGtpLastNoRespToEchoGSNIpAddr | Sent when a GGSN peer (SGSN or charging gateway) fails to respond to the GTP echo request message for the time period of the N3-requests counter configured using the gprs gtp n3-requests global configuration command. Enable the generation of this notification by setting the cGtpNotifEnable to true(1). |

Alarm Notifications

Depending on the severity level, notifications are considered alarms or informational events. Notifications with a severity level of critical, major, or minor are classified as alarms. An alarm must be reported when an alarm state changes (assuming the alarm does not have a nonreported severity).

Informational events do not require state changes. An informational event is a warning that an abnormal condition that does not require corrective action has occurred. The informational event needs to be reported but is transient. No corrective action is required to fix the problem.

Table A-6 lists the severity levels and the required responses.

Table A-6 *Notification Severity Levels*

| Severity Level | Description |
|----------------|--|
| Critical | A serious condition exists. If an action is recommended, clear critical alarms immediately. |
| Major | A disruption of service has occurred. Clear this alarm immediately. |
| Minor | No disruption of service has occurred, but clear this alarm as soon as possible. |
| Informational | A warning that an abnormal condition that does not require corrective action has occurred. An informational event is reported but is transient. No corrective action is required by the management center to fix this problem. |

Alarms have a trap type associated with them. Table A-7 identifies the trap types that can be associated with an Alarm.

Table A-7 *Alarm Trap Types*

| Trap Type | Description |
|-------------------|---|
| 1 (cleared) | Indicates a previous alarm condition has been cleared. It is not required, unless specifically stated elsewhere on a case-by-case basis, that an alarm condition that has been cleared will produce a notification or other event containing an alarm severity with this value. |
| 2 (indeterminate) | Indicates that the severity level cannot be determined. |

Table A-7 Alarm Trap Types

| Trap Type | Description |
|--------------|---|
| 3 (critical) | A service-affecting condition has occurred and an immediate action is possibly required. |
| 4 (major) | A service-affecting condition has occurred and an urgent corrective action is possibly required. |
| 5 (minor) | A nonservice-affecting condition exists and corrective action should be taken in order to prevent a more serious condition (for example, a safety-affecting condition). |
| 6 (warning) | A potential or impending service or safety affection condition has been detected before any significant affects have been felt. |
| 7 (info) | The alarm condition does not meet any other severity definition. This can include important, but non--urgent notices or informational events. |

The following sections describe alarms supported by the following notifications:

- [cGgsnGlobalErrorNotif](#), page A-48
- [cGgsnAccessPointNameNotif](#), page A-50
- [CgprsCgAlarmNotif](#), page A-53
- [cgprsAccPtCfgNotif](#), page A-55

cGgsnGlobalErrorNotif

[Table A-8](#) lists alarms supported by the cGgsnGlobalErrorNotif notification (CISCO-GGSN-MIB). Alarms supported by the cGgsnGlobalErrorNotif notification are global-related alarms.

Table A-8 cGgsnGlobalErrorNotif Alarms

| Alarm | Description |
|---------------|--|
| ggsnServiceUp | <p>Cause: GGSN service has been started. The service gprs global configuration command has been issued.</p> <p>Severity Level and Trap Type: The severity level is critical. The trap type is 3.</p> <p>Recommended Action: This is an informational event. No action is required.</p> |

Table A-8 cGgsnGlobalErrorNotif Alarms

| Alarm | Description |
|-----------------|--|
| ggsnServiceDown | <p>Cause: GGSN service is down. The no gprs service global configuration command has been issued or the system service is down because of another reason.</p> <p>Severity Level and Trap Type: The severity level is critical. The trap type is 3.</p> <p>Recommended Action: Attempt to restart the GGSN service on the router by issuing the service gprs global configuration command and if the problem persists, contact your Cisco technical support representative with the error message.</p> |
| noDHCPsServer | <p>Cause: A DHCP server is not configured. This error notification is generated when part of the DHCP server configuration is missing or is incorrect.</p> <p>Severity Level and Trap Type: The severity level is major. The trap type is 4.</p> <p>Recommended Action: Ensure that all elements of the DHCP configuration are properly configured.</p> |

cGgsnAccessPointNameNotif

Table A-9 lists alarms supported by the cGgsnAccessPointNameNotif notification (CISCO-GGSN-MIB). Alarms supported by the cGgsnAccessPointNameNotif notification are APN-related alarms.

Table A-9 *cGgsnAccessPointNameNotif Alarms*

| Alarm | Description |
|-----------------|---|
| noRadius | <p>Cause: A RADIUS server is not configured. This error notification is generated when part of the RADIUS server configuration is missing.</p> <p>Severity Level and Trap Type: The severity level is major. The trap type is 4.</p> <p>Recommended Actions:</p> <ol style="list-style-type: none"> 1. Verify that the RADIUS server is properly configured and that you can ping it. 2. Ensure that the RADIUS server is configured properly. 3. Note the error message, issue a show running configuration and contact your Cisco technical support representative. |

Table A-9 cGsnAccessPointNameNotif Alarms (continued)

| Alarm | Description |
|-------------------------|--|
| ipAllocationFail | <p>Cause: Dynamic IP allocation failed because of one of the following reasons:</p> <ol style="list-style-type: none"> 1. One of the following DHCP or RADIUS server problem might have occurred: <ol style="list-style-type: none"> a. The DHCP/RADIUS server IP address is configured incorrectly in the GGSN. b. The DHCP/RADIUS server is reachable, but the configuration to allocate IP addresses might be incorrect. c. The DHCP or RADIUS server is properly configured, but cannot be reached. 2. Dynamic IP allocation is disabled in the APN configuration. 3. The PAP or CHAP username and password information is missing from the RADIUS client in transparent mode. Therefore, this information is missing in the PDP activation request. <p>Severity Level and Trap Type: The severity level is major. The trap type is 4.</p> <p>Recommended Actions:</p> <ol style="list-style-type: none"> 1. Check the DHCP/RADIUS server configuration, ensuring that: <ol style="list-style-type: none"> a. The DHCP/RADIUS server IP address configured on the GGSN is valid. b. The DHCP/RADIUS server is properly configured to allocate IP addresses. c. The DHCP/RADIUS server is reachable (via the ping command). 2. Configure IP allocation pool in the APN as either DHCP proxy client or RADIUS client. 3. If none of the above does not resolve the alarm condition, contact you Cisco technical support representative with the error message. |
| apnUnreachable | <p>Cause: A PDP activation has failed because the APN requested in the create PDP context request is not configured on the GGSN.</p> <p>Severity Level and Trap Type: The severity level is major. The trap type is 4.</p> <p>Recommended Action: Check the configuration of the corresponding APN. If the configuration appears to be correct, contact your Cisco technical support representative with the error message and saved output of the show running-config and show gprs access-point all commands.</p> |

cGgsnPacketDataProtocolNotif

Table A-10 lists alarms supported by the cGgsnPacketDataProtocolNotif notification (CISCO-GGSN-MIB). Alarms supported by the cGgsnPacketDataProtocolNotif notification are PDP-related alarms.

Table A-10 cGgsnPacketDataProtocolNotif Alarms

| Alarm | Description |
|---------------------------|---|
| noResource | <p>Cause: Resources available to continue GGSN service are exhausted because of one of the following reasons:</p> <ol style="list-style-type: none"> 1. Maximum number of PDP contexts has been reached. 2. Maximum number of PPP-regenerated PDP contexts has been reached. <p>Severity Level and Trap Type: The severity level is critical. The trap type is 3.</p> <p>Recommended Action: If possible, increase the number of PDP contexts that can be processed by the GGSN. If the problem persists, contact your Cisco technical support representative with the error message.</p> |
| authenticationFail | <p>Cause: A PDP activation has failed because of one of the following reasons:</p> <ol style="list-style-type: none"> 1. There is no RADIUS server present for authentication because a RADIUS server is not configured or is unreachable. 2. An invalid username or password is used in the create PDP context request. 3. The PAP/CHAP information element is missing in the create PDP context request in non-transparent mode. 4. The username is not present in the create PDP context request. 5. There is a duplicate IP address to access the APN. <p>Severity Level and Trap Type: The severity level is warning. The trap type is 6.</p> <p>Recommended Action: Verify that the RADIUS server is configured properly and is reachable using the ping command. If it is, contact your Cisco technical support representative with the error message and the saved output of the show running-config.</p> |

CgprsCgAlarmNotif

Table A-11 lists alarms supported by the CgprsCgAlarmNotif notification (CISCO-GPRS-CHARGING-MIB). Alarms supported by the CgprsCgAlarmNotif notification are alarms related to the charging functions of the GGSN.

Table A-11 CgprsCgAlarmNotif Alarms

| Alarm | Description |
|---------------------------------|---|
| cgprsCgAlarmCgDown | <p>Cause: The charging gateway (primary, secondary, and tertiary) is down because it is not configured or there is a missing response to a nodealive request on the charging gateway path.</p> <p>Severity Level and Trap Type: The severity level is critical. The trap type is 3.</p> <p>Recommended Action: Verify that a charging gateway configuration exists and that the correct IP address is assigned. If it is, then the charging gateway is down.</p> |
| cgprsCgAlarmCgUp | <p>Cause: The charging gateway is up.</p> <p>Severity Level and Trap Type: The severity level is critical. The trap type is 3.</p> <p>Recommended Action: This is an informational event. No action is required.</p> |
| cgprsCgAlarmTransFailure | <p>Cause: The GGSN has repeatedly failed to receive a response from the charging gateway for data record transfer requests.</p> <p>Severity Level and Trap Type: The severity level is critical. The trap type is 3.</p> <p>Recommended Action: Verify that the charging gateways are properly configured on the GGSN and charging functionality is active.</p> |
| cgprsCgAlarmTransSuccess | <p>Cause: The GGSN has successfully sent data record transfer requests to the charging gateway after the failure.</p> <p>Severity Level and Trap Type: The severity level is critical. The trap type is 3.</p> <p>Recommended Action: This is an informational event. No action is required.</p> |
| cgprsCgAlarmCapacityFull | <p>Cause: The GGSN buffer is full and subsequent packets might be dropped.</p> <p>Severity Level and Trap Type: The severity level is critical. The trap type is 3.</p> <p>Recommended Action: Confirm the value configured for the gprs charging send-buffer global configuration command, and if possible, increase the number of bytes configured for the buffer.</p> |

Table A-11 CgprsCgAlarmNotif Alarms (continued)

| Alarm | Description |
|--------------------------------------|--|
| cgprsCgAlarmCapacityFree | <p>Cause: The GGSN is able to buffer G-CDR after a failure to buffer G-CDRs has occurred.</p> <p>Severity Level and Trap Type: The severity level is critical. The trap type is 3.</p> <p>Recommended Action: This is an informational event. No action is required.</p> |
| cgprsCgAlarmEchoFailure | <p>Cause: The GGSN has failed to receive an echo response from the charging gateway to an echo request.</p> <p>Severity Level and Trap Type: The severity level is critical. The trap type is 3.</p> <p>Recommended Action: Verify that the charging gateways are properly configured on the GGSN. If the condition persists, contact your Cisco technical support representative with the error message.</p> |
| cgprsCgAlarmEchoRestored | <p>Cause: The GGSN has received an echo response from the charging gateway after an cgprsCgAlarmEchoFailure was sent.</p> <p>Severity Level and Trap Type: The severity level is critical. The trap type is 3.</p> <p>Recommended Action: This is an informational event. No action required.</p> |
| cgprsCgAlarmChargingDisabled | <p>Cause: Indicates that charging transactions on the GGSN are disabled.</p> <p>Severity Level and Trap Type: The severity level is critical. The trap type is 3.</p> <p>Recommended Action: This is an informational event. No action is required.</p> |
| cgprsCgAlarmChargingEnabled | <p>Cause: Indicates that charging transactions on the GGSN are enabled.</p> <p>Severity Level and Trap Type: The severity level is critical. The trap type is 3.</p> <p>Recommended Action: This is an informational event. No action is required.</p> |
| cgprsCgGatewaySwitchoverNotif | <p>Cause: Indicates that the active charging gateway has switched.</p> <p>Recommended Action: This is an informational event. Determine why the charging gateway switchover occurred.</p> |

Table A-11 CgprsCgAlarmNotif Alarms (continued)

| Alarm | Description |
|-----------------------------|---|
| cgprsCgInServiceModeNotif | <p>Cause: Indicates that the GGSN charging function has been placed in in-service/operational mode from maintenance mode.</p> <p>Recommended Action: This is an informational event. No action is required.</p> |
| cgprsCgMaintenanceModeNotif | <p>Cause: Indicates that the GGSN charging function has been placed in maintenance mode from in-service/operational mode.</p> <p>Recommended Action: This is an informational event. No action is required.</p> |

cgprsAccPtCfgNotif

Table A-12 lists alarms supported by the cgprsAccPtCfgNotif notification (CISCO-GPRS-ACC-PT-MIB).

Table A-12 cgprsAccPtCfgNotif

| Alarm | Description |
|--------------------|---|
| cgprsAccPtCfgNotif | <p>Cause: The access point configuration has been created, modified, or deleted.</p> <p>Severity Level and Trap Type: Not applicable</p> <p>Recommended Action: This is an informational event. No action is required.</p> |

