



Monitoring Notifications

This appendix describes enabling and monitoring CSG2 SNMP notifications in order to manage CSG2-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 CSG2 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 12.4 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 F-1](#)
- [Configuring MIB Support, page F-6](#)
- [Enabling SNMP Support, page F-8](#)
- [Enabling and Disabling SNMP Notifications, page F-9](#)

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 F-8).
- **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.

For a list of all MIBs supported by the CSG2 Release 2, see the [“MIB Support”](#) section on page 1-5.

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 F-8](#) for instructions on how to enable traps on the CSG2.

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 6-1 describes the security models and levels provided by the different SNMP versions.

Table 6-1 *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/ios120/12cger/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 F-6
- [Downloading and Compiling MIBs](#), page F-6
- [Enabling SNMP Support](#), page F-8

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-SAMI**. 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 CSG2 release.
 - b. By image name—From the MIB Locator page, enter the CSG2 image name you are using in the Search by Image Name field and click **Submit**.
 - 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 CSG2:

- [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, you must set up your basic SNMP configuration through the command line interface (CLI) on the router.



Note

These basic configuration commands are for SNMPv2c. For SNMPv3, you must also set up SNMP users and groups. (See the preceding list of documents for command and setup information.)

Step 1 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
```

Step 2 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 SNMP Notifications

To enable and disable SNMP Notifications, perform the tasks in the following sections:

- [Enabling and Disabling CSG2 Notifications via the CLI, page F-9](#)
- [Enabling and Disabling CSG2 SNMP Notifications via SNMP, page F-10](#)

Enabling and Disabling CSG2 Notifications via the CLI

To use the command line interface (CLI) to enable the Cisco router to send CSG2 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 F-8).

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 CSG2 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 csg [bma [records | state] | database |
quota-server [records | state]]
```

Where:

- **bma**—Enables traps for only the Billing Mediation Agents (BMAs) to which the CSG2 sends billing records.
 - **records**—Enables only lost records traps for the BMAs.
 - **state**—Enables only state change traps for the BMAs.
- **database**—Enables traps for only the database server that answers CSG2 user ID queries.
- **quota-server**—Enables traps for only the CSG2 quota servers.
 - **records**—Enables only lost records traps for the quota servers.
 - **state**—Enables only state change traps for the quota servers.



Note Entering the `snmp-server enable traps csg` command without a keyword option enables all CSG2 SNMP notifications.

Step 4 To disable CSG2 SNMP notifications on the Cisco router, enter the following command.

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

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

Enabling and Disabling CSG2 SNMP Notifications via SNMP



Note

The set operation is not yet valid for these objects. We recommend that you use the CLI to enable and disable CSG2 SNMP notifications.

Additionally, CSG2 SNMP Notifications can be enabled or disabled by setting the following objects to true(1) or false(2).

- `ccsBMASharedStateChangeNotifEnabled`—Enables/disables the generation of the Billing Mediation Agent (BMA) state change notification (`ciscoContentServicesBMASharedStateChange`)
- `ccsQuotaMgrStateChangeNotifEnabled`—Enables/disables the generation of the Quota Manager state change notification (`ciscoContentServicesQuotaMgrStateChange`)
- `ccsUserDbStateChangeNotifEnabled`—Enables/disables the generation of the User Database Server state change notification (`ciscoContentServicesUserDbStateChange`)
- `ccsBMALostRecordEventNotifEnabled`—Enables/disables the generation of the Billing Mediation Agent Lost Record notification (`ciscoContentServicesBMALostRecordEvent`)
- `ccsQuotaMgrLostRecordEventNotifEnabled`—Enables/disables the generation of the Quota Manager Lost Record notification (`ciscoContentServicesQuotaMgrLostRecordEvent`)