SNMP Software Configuration Guide for Cisco 1000 Series Connected Grid Routers (Cisco IOS)

January 2014
OL-31243-01

This chapter describes how to configure Simple Network Management Protocol (SNMP) on the Cisco 1000 Series Connected Grid Router (hereafter referred to as the CGR 1000).

This chapter includes the following sections:

Information About SNMP

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.

This section includes the following topics:

Cisco Systems, Inc.
www.cisco.com

SNMP Functional Overview

The SNMP framework consists of three parts:

- An SNMP manager—The system used to control and monitor the activities of network devices using SNMP.
- An SNMP agent—The software component within the managed device that maintains the data for the device and reports these data, as needed, to managing systems. To enable the SNMP agent, you must define the relationship between the manager and the agent.
- A managed information base (MIB)—The collection of managed objects on the SNMP agent.

The CGR 1000 supports SNMP over IPv4 and IPv6. You can configure the CGR 1000 as SNMP agent and SNMP manager.

SNMP Versions

The CGR 1000 software supports the following versions of SNMP:

- SNMPv1—Simple Network Management Protocol: a full Internet standard, defined in RFC 1157. (RFC 1157 replaces the earlier versions that were published as RFC 1067 and RFC 1098.) Security is based on community strings.
- SNMPv2c—The community string-based Administrative Framework for SNMPv2. SNMPv2c (the "c" is for "community") is an experimental Internet protocol defined in RFC 1901, RFC 1905, and RFC 1906. 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 is an interoperable standards-based protocol defined in RFCs 3413 to 3415. SNMPv3 provides secure access to devices by authenticating and encrypting packets over the network. In SNMPv3, an authentication strategy is set up for a user and the group in which the user resides.

Security Models and Levels

Three security models are available: SNMPv1, SNMPv2c, and SNMPv3.

The security level determines if an SNMP message needs to be protected from disclosure and if the message needs to be authenticated. The various security levels that exist within a security model are as follows:

- noAuthNoPriv—Security level that does not provide authentication or encryption.
- authNoPriv—Security level that provides authentication but does not provide encryption.
- authPriv—Security level that provides both authentication and encryption.

The security model combined with the security level determine the security mechanism applied when the SNMP message is processed.

Table 1 lists the combinations of security models and levels and their meanings.

Table 1 SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)	No	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
v3	authPriv	MD5 or SHA	Data Encryption Standard (DES), 3-DES, and Advanced Encryption Standard (AES)	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit, 3-DES, or AES encryption in addition to authentication.

User-Based Security Model

The SNMPv3 User-Based Security Model (USM) refers to SNMP message-level security and offers the following services:

- Message integrity—Ensures that messages have not been altered or destroyed in an unauthorized manner and that data sequences have not been altered to an extent greater than can occur non-maliciously.
- Message origin authentication—Ensures that the claimed identity of the user on whose behalf received data was originated is confirmed.
- Message confidentiality—Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

SNMPv3 authorizes management operations only by configured users and encrypts SNMP messages.

The CGR 1000 uses two authentication protocols for SNMPv3:

- HMAC-MD5-96 authentication protocol
- HMAC-SHA-96 authentication protocol

The CGR 1000 supports DES 56-bit, 3-DES, or AES as the privacy protocol for SNMPv3 message encryption.

SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. These notifications do not require that requests be sent from the SNMP manager. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of a connection to a neighbor router, or other significant events.

CGR 1000 generates SNMP notifications as either traps or informs. A trap is an asynchronous, unacknowledged message sent from the agent to the SNMP managers listed in the host receiver table. Informs are asynchronous messages sent from the SNMP agent to the SNMP manager which the manager must acknowledge receipt of.

Traps are less reliable than informs because the SNMP manager does not send any acknowledgment when it receives a trap. The CGR 1000 cannot determine if the trap was received. An SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the CGR 1000 never receives a response, it can send the inform request again.

You can configure the CGR 1000 to send notifications to multiple host receivers. See the section Configuring a Recipient of an SNMP Trap Operation in the SNMP Configuration Guide, Cisco IOS Release 15M&T for more information about host receivers.

Note Many **snmp-server** commands use the keyword **traps** in their command syntax. Unless there is an option within the command to specify either traps or informs, the keyword **traps** should be taken to mean traps, informs, or both. Use the **snmp-server host** command to specify whether you want SNMP notifications to be sent as traps or informs. To use informs, the SNMP manager (also known as the SNMP proxy manager) must be available and enabled on a device.

Table 2 lists the notifications that the CGR 1000 supports, the associated MIBs, and the commands to enable the notifications.

Note The MIBs shown in Table 2 are supported only for the associated notification. The complete MIBs and associated notifications that the CGR 1000 supports are listed in Table 3.

Table 2 CGR 1000 Notifications

Notification	MIB	Command
cafAuthFailNotif	CISCO-AUTH-FRAMEWORK-MIB	**snmp-server enable traps auth-framework auth-fail**
cefcModuleStatusChange	CISCO-ENTITY-FRU-CONTROL-MIB	**snmp-server enable traps fru-ctrl**
entSensorThresholdNotification	CISCO-ENTITY-SENSOR-MIB	**snmp-server enable traps entity-sensor threshold**
entSensorThresholdRecoveryNotification		
ciscoEnvMonEnableStatChangeNotif	CISCO-ENVMON-MIB	**snmp-server enable traps envmon fan**
		snmp-server enable traps envmon shutdown
		snmp-server enable traps envmon status
		snmp-server enable traps envmon supply
		snmp-server enable traps envmon temperature
		snmp-server enable traps envmon voltage

Table 2 CGR 1000 Notifications (continued)

Notification	MIB	Command
ciscoFlashLowSpaceNotif	CISCO-FLASH-MIB	**snmp-server enable traps flash low-space**
ciscoFlashLowSpaceRecoveryNotif		**snmp-server enable traps flash removal**
ciscoFlashDeviceRemovedNotifRev1		**Note** When the flash is removed, ciscoFlashDeviceRemovedNotifRev1 is generated (if enabled) and the CGR 1000 reboots. Flash insertion notifications are not supported.
ciscoSystemHeartBeatNotif	CISCO-SYSTEM-MIB	**snmp-server enable traps cisco-sys heartbeat** **Note** To enable heartbeat notifications, you must also configure the heartbeat interval and set the heartbeat state to active. See the "Configuring Heartbeat Notifications" section on page 8.
ceExtEntDoorCloseNotif	CISCO-ENTITY-EXT-MIB	**snmp-server enable traps entity-ext**
ceExtEntDoorOpenNotif		
cefcFRURemoved	CISCO-ENTITY-FRU-CONTROL	**snmp-server enable traps fru-ctrl**
cefcFRUInserted		
ciscoMemoryPoolLowMemoryNotif	CISCO-MEMORY-POOL-MIB	**snmp-server enable traps mempool**
ciscoMemoryPoolLowMemoryRecoveryNotif(2)		

Supported MIBs

Table 3 lists the MIBs that the CGR 1000 supports and the commands to enable notifications for the MIBs.

Table 3 CGR 1000 MIBs

MIB	Related commands
SYSTEM	There are no traps for this MIB.
IF-MIB	**snmp-server enable traps link** **snmp-server enable traps link linkDown** **snmp-server enable traps link linkUp**
ENTITY-MIB	There are no traps for this MIB.

Table 3 CGR 1000 MIBs (continued)

MIB	Related commands
CISCO-WAN-3G-MIB	**snmp-server enable traps c3g** **Note** See *Cisco Connected Grid Cellular 3G GSM Module for CGR 1000 Series Installation and Configuration Guide (Cisco IOS)* for commands to enable specific GSM event traps. See *Cisco Connected Grid Cellular 3G CDMA Module for CGR 1000 Series Installation and Configuration Guide (Cisco IOS)* for commands to enable specific CDMA event traps.
SNMPv2-MIB	**snmp-server enable traps snmp** **snmp-server enable traps snmp authentication**
CISCO-AAA-SERVER-MIB	**snmp-server enable traps aaa_server**
CISCO-NTP-MIB	There are no traps for this MIB.
CISCO-CONFIG-COPY-MIB	**snmp-server enable traps config-copy**
CISCO-IMAGE-MIB	There are no traps for this MIB.
CISCO-FLASH-MIB	**snmp-server enable traps flash**
SNMP-NOTIFICATION-MIB	There are no traps for this MIB.
SNMP-MPD-MIB	There are no traps for this MIB.
CISCO-PROCESS-MIB	**snmp-server enable traps cpu threshold**
SNMP-FRAMEWORK-MIB	There are no traps for this MIB.
CISCO-IF-EXTENION-MIB	There are no traps for this MIB.

Cisco MIB Locator

To locate and download the MIBs for the CGR 1000, visit the Cisco MIB Locator page:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

Prerequisites

SNMP versions 1 and 2:

- An established SNMP community string that defines the relationship between the SNMP manager and the agent.
- A host defined to be the recipient of SNMP notifications.

SNMP version 3:

- The network management station (NMS) must support SNMP version 3 to be able to use SNMP version 3 encryption.

- SNMP version 3 encryption is available only in Cisco software images that support encryption algorithms.
- You should have an understanding of the security model used and how the security model interacts with the other subsystems in the SNMP architecture.

Guidelines and Limitations

- For the router that runs the SNMP agent, you must configure appropriate access control (for example, SNMP-server community) using the Cisco IOS CLI for the NMS and agent to work properly.
- It is strongly recommended that you configure SNMPv3 with authentication/privacy when implementing SNMP SET operation.

Default Settings

By default, SNMP is not enabled. Required traps must be enabled as described in the section Configuring SNMP Notifications in the SNMP Configuration Guide, Cisco IOS Release 15M&T. See Table 3 for the commands to enable notifications on the CGR 1000.

Configuring SNMP

There is no specific command that you use to enable SNMP. The first **snmp-server** command that you enter enables the supported versions of SNMP. All other configurations are optional.

To configure SNMP support on the CGR 1000, perform these tasks in the section How to Configure SNMP Support in the SNMP Configuration Guide, Cisco IOS Release 15M&T:

- Configuring System Information
- Configuring SNMP Versions 1 and 2
- Configuring SNMP Version 3
- Configuring a Device as an SNMP Manager
- Enabling the SNMP Agent Shutdown Mechanism
- Defining the Maximum SNMP Agent Packet Size
- Limiting the Number of TFTP Servers Used via SNMP
- Disabling the SNMP Agent
- Configuring SNMP Notifications

To configure heartbeat notifications on the CGR 1000, follow the procedure in the next section.

Configuring Heartbeat Notifications

Follow this procedure to configure the CGR 1000 to generate heartbeat notifications.

BEFORE YOU BEGIN

Review the information in the "SNMP Notifications" section on page 3.

DETAILED STEPS

	Command	Purpose
Step 1	**cgna heart-beat interval** *interval*	Sets the interval for generating the heartbeat notification. *interval*—1–6000 minutes
Step 2	**cgna heart-beat active**	Sets the heartbeat state to active.
Step 3	**snmp-server enable traps cisco-sys heartbeat**	Enable heartbeat notifications.

To disable the heartbeat, use the **no cgna heart-beat active** command.

EXAMPLE

```
Router(config)#cgna heart-beat interval 5
Router(config)#cgna heart-beat active
Router(config)#snmp-server enable traps cisco-sys heartbeat
```

Verifying Configuration

Command	Purpose
show snmp	Displays the status of SNMP communications.
show snmp engineID [**local** | **remote**]	Displays information about the local SNMP engine and all remote engines that have been configured on the device.
show snmp sessions [**brief**]	Displays information about current sessions.
show snmp pending	Displays information about current pending requests.
show snmp group	Displays information about each SNMP group on the network.
show snmp user	Displays information about the configured characteristics of SNMP users.

To monitor SNMP trap activity in real time for the purposes of troubleshooting, use the SNMP **debug** commands, including the **debug snmp packet** EXEC command. For documentation of SNMP **debug** commands, see the *Cisco IOS Debug Command Reference*.

Configuration Example

See the section Example Configuring SNMPv1 SNMPv2c and SNMPv3 in the SNMP Configuration Guide, Cisco IOS Release 15M&T for SNMP configuration examples.

Related Documents

- SNMP Configuration Guide, Cisco IOS Release 15M&T
- Cisco IOS SNMP Support Command Reference

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

This document is to be used in conjunction with the documents listed in the "Related Documents" section.