Configuring SNMP

This chapter describes how to configure the SNMP feature on Cisco CG-OS routers.

This chapter includes the following sections:

- Information About SNMP, page 3-1
- Cisco MIB Locator, page 3-5
- Default Settings, page 3-5
- Configuring SNMP, page 3-6
- Verifying Configuration, page 3-19
- Configuration Examples, page 3-20
- Useful Common MIBs, page 3-21
- Feature History, page 3-21

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:

- SNMP Functional Overview, page 3-2
- SNMP Notifications, page 3-2
- SNMPv3, page 3-3

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. Cisco CG-OS supports the agent and MIB. 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.

SNMP is defined in RFCs 3411 to 3418.

Cisco CG-OS supports SNMPv2c, and SNMPv3. SNMPv2c uses a community-based form of security.

Cisco CG-OS supports SNMP over IPv4 and IPv6.

Note CG-OS does not support multiple VDCs. It always uses the default VDC (VDC 1).

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.

Cisco CG-OS 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. Cisco CG-OS 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 Cisco CG-OS never receives a response, it can send the inform request again.

You can configure Cisco CG-OS to send notifications to multiple host receivers. See the "Configuring SNMP Notification Receivers" section on page 3-10 for more information about host receivers.

SNMPv3

SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. The security features provided in SNMPv3 are as follows:

- Message integrity—Ensures that a packet has not been tampered with while it was in-transit.
- Authentication—Determines that the message is from a valid source.
- Encryption—Scrambles the packet contents to prevent it from being seen by unauthorized sources.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

This section includes the following topics:

- Security Models and Levels for SNMPv2, v3, page 3-3
- User-Based Security Model, page 3-4
- CLI and SNMP User Synchronization, page 3-4
- Group-Based SNMP Access, page 3-5

Security Models and Levels for SNMPv2, v3

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.

Three security models are available: SNMPv2c, and SNMPv3. The security model combined with the security level determine the security mechanism applied when the SNMP message is processed.

Table 3-1 identifies what the combinations of security models and levels mean.

Table 3-1 SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v3	authNoPriv	HMAC-MD5 or HMAC-SHA	No	Provides authentication based on the Hash-Based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm or the HMAC Secure Hash Algorithm (SHA).
v3	authPriv	HMAC-MD5 or HMAC-SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.

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 nonmaliciously.
- 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.

Cisco CG-OS uses two authentication protocols for SNMPv3:

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

Cisco CG-OS uses Advanced Encryption Standard (AES) as one of the privacy protocols for SNMPv3 message encryption and conforms with RFC 3826.

The **priv** option offers a choice of DES or 128-bit AES encryption for SNMP security encryption. The **priv** option and the **aes-128** token indicate that this privacy password is for generating a 128-bit AES key.The AES priv password can have a minimum of eight characters. If the passphrases are specified in clear text, you can specify a maximum of 64 case-sensitive alphanumeric characters. If you use the localized key, you can specify a maximum of 130 characters.

Note For an SNMPv3 operation that uses the external AAA server, you must use AES for the privacy protocol in the user configuration on the external AAA server.

CLI and SNMP User Synchronization

SNMPv3 user management can be centralized at the Access Authentication and Accounting (AAA) server level. This centralized user management allows the SNMP agent in Cisco CG-OS to leverage the user authentication service of the AAA server. Once user authentication is verified, the SNMP PDUs are processed further. Additionally, the AAA server is also used to store user group names. SNMP uses the group names to apply the access/role policy that is locally available in the router.

Any configuration changes made to the user group, role, or password results in database synchronization for both SNMP and AAA.

Cisco CG-OS synchronizes user configuration in the following ways:

- The authentication passphrase specified in the **snmp-server user** command becomes the password for the CLI user.
- The password specified in the **username** command becomes the authentication and privacy passphrases for the SNMP user.
- If you create or delete a user using either SNMP or the CLI, the user is created or deleted for both SNMP and the CLI.
- User-role mapping changes are synchronized in SNMP and the CLI.
- Role changes (deletions or modifications) from the CLI are synchronized to SNMP.

Note When you configure a passphrase/password in localized key/encrypted format, Cisco CG-OS does not synchronize the user information (password, roles, and so on).

Cisco CG-OS holds the synchronized user configuration for 60 minutes by default. See the "Modifying the AAA Synchronization Time" section on page 3-18 for information on how to modify this default value.

Group-Based SNMP Access

Note Because *group* is a standard SNMP term used industry-wide, we refer to role(s) as group(s) in this SNMP section.

SNMP access rights are organized by groups. Each group in SNMP is similar to a role through the CLI. Each group is defined with read access or read-write access.

You can begin communicating with the agent once your username is created, your roles are set up by your administrator, and you are added to the roles.

Cisco MIB Locator

To locate and download the MIBs supported by Cisco CG-OS, visit the Cisco MIB Locator page:

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

For a list of supported MIBs and MIB notifications, see Table 3-3.

Default Settings

Table 3-2 lists the default settings for SNMP parameters.

Table 3-2 Default SNMP Parameters

Parameters	Default
LinkUp/LinkDown Notifications	Enabled
Module inserted/removed Notifications	Enabled

Configuring SNMP

This section includes the following topics:

- Configuring SNMP Users, page 3-7
- Enforcing SNMP Message Encryption, page 3-7
- Assigning SNMPv3 Users to Multiple Roles, page 3-8
- Creating SNMP Communities, page 3-8
- Filtering SNMP Requests, page 3-9
- Configuring SNMP Notification Receivers, page 3-10
- Configuring a Source Interface for SNMP Notifications, page 3-11
- Configuring the Notification Target User, page 3-12
- Configuring SNMP to Send Traps Using an Inband Port, page 3-12
- Enabling SNMP Notifications, page 3-14
- Displaying SNMP ifIndex for an Interface, page 3-16
- Disabling LinkUp/LinkDown Notifications on an Interface, page 3-15
- Enabling a One-time Authentication for SNMP over TCP, page 3-16
- Assigning the SNMP Device Contact and Location Information, page 3-17
- Configuring the Context to Network Entity Mapping, page 3-17
- Disabling SNMP, page 3-18
- Modifying the AAA Synchronization Time, page 3-18

Configuring SNMP Users

You can configure a user for SNMP.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Router enters global configuration mode.
Step 2	**snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*] [**localizedkey**]]	Configures an SNMP user with authentication and privacy parameters. The passphrase can be any case-sensitive alphanumeric string up to 64 characters. If you use the **localizedkey** keyword, the passphrase can be any case-sensitive alphanumeric string up to 130 characters. The engineID format is a 12-digit colon-separated decimal number.
Step 3	**show snmp user**	(Optional) Displays information about one or more SNMP users.
Step 4	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to configure the SNMP contact and location information:

```
router# configure terminal
router(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh
router(config-callhome)# show snmp user
router(config)# copy running-config startup-config
```

Enforcing SNMP Message Encryption

You can configure SNMP to require authentication or encryption for incoming requests. By default, the SNMP agent accepts SNMPv3 messages without authentication and encryption. When you enforce privacy, Cisco CG-OS responds with an authorizationError for any SNMPv3 PDU request using securityLevel parameter of either noAuthNoPriv or authNoPriv.

Use the following command in global configuration mode to enforce SNMP message encryption for a user:

Command	Purpose
snmp-server user *name* **enforcePriv** **Example:** router(config)# **snmp-server user Admin enforcePriv**	Enforces SNMP message encryption for this user.

Use the following command in global configuration mode to enforce SNMP message encryption for all users:

Command	Purpose
snmp-server globalEnforcePriv **Example:** router(config)# **snmp-server globalEnforcePriv**	Enforces SNMP message encryption for all users.

Assigning SNMPv3 Users to Multiple Roles

After you configure an SNMP user, you can assign multiple roles for the user.

Note Only users belonging to a network-admin role can assign roles to other users.

Use the following command in global configuration mode to assign a role to an SNMP user:

Command	Purpose
snmp-server user *name group* **Example:** router(config)# **snmp-server user Admin superuser**	Associates this SNMP user with the configured user role.

Creating SNMP Communities

You can create SNMP communities for SNMPv2c.

Use the following command in global configuration mode to create an SNMP community string:

Command	Purpose
snmp-server community *name group* **{ro | rw}** **Example:** router(config)# **snmp-server community public ro**	Creates an SNMP community string.

Filtering SNMP Requests

You can assign an access list (ACL) to a community to filter incoming SNMP requests. If the assigned ACL allows the incoming request packet, SNMP processes the request. If the ACL denies the request, SNMP drops the request and sends a system message.

Create the ACL with the following parameters:

- Source IP address
- Destination IP address
- Source port
- Destination port
- Protocol (UDP or TCP)

See the *Cisco 1000 Series Connected Grid Routers Security Software Configuration Guide* for more information on creating ACLs. The ACL applies to IPv4 over UDP and TCP.

Use the following command in global configuration mode to assign an ACL to a community to filter SNMP requests:

Command	Purpose
snmp-server community *community-name* **use-acl** *acl-name* **Example:** `router(config)# snmp-server community public use-acl my_acl_for_public`	Assigns an ACL to an SNMP community to filter SNMP requests.

Configuring SNMP Notification Receivers

You can configure Cisco CG-OS to generate SNMP notifications to multiple SNMPv2c and SNMPv3 host receivers.

Use the following command in global configuration mode to configure a host receiver for SNMPv2c traps or informs:

Command	Purpose
snmp-server host *ip-address* **{traps | informs} version 2c** *community* [**udp_port** *number*] **Example:** `router(config)# snmp-server host 192.0.2.1 informs version 2c public`	Configures a host receiver for SNMPv2c traps or informs. The *ip-address* can be an IPv4 or IPv6 address, or a domain name. The *community* can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

Use the following command in global configuration mode to configure a host receiver for SNMPv3 traps or informs:

Command	Purpose
snmp-server host *ip-address* **{traps | informs} version 3 {auth | noauth | priv}** *username* **[udp_port number** *port***]** **Example:** `router(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS`	Configures a host receiver for SNMPv3 traps or informs. The *ip-address* can be an IPv4 or IPv6 address, or a domain name. The *username* can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

Note The SNMP manager must know the user credentials (authKey/PrivKey) based on the SNMP engine ID of the Cisco CG-OS device to authenticate and decrypt the SNMPv3 messages.

Configuring a Source Interface for SNMP Notifications

You can configure SNMP to use the IP address of an interface as the source IP address for notifications. When a notification is generated, its source IP address is based on the IP address of this configured interface. You can configure this as follows:

- All notifications sent to all SNMP notification receivers.
- All notifications sent to a specific SNMP notification receiver. This configuration overrides the global source interface configuration.

Note Configuring the source interface IP address for outgoing trap packets does not guarantee that the device will use the same interface to send the trap. The source interface IP address defines the source address inside of the SNMP trap, and the connection is opened with the address of the egress interface as source.

Use the following command in global configuration mode to configure a host receiver on a source interface:

Command	Purpose
snmp-server host *ip-address* **source-interface** *if-type if-number* [**udp_port** *port*] **Example:** `router(config)# snmp-server host 192.0.2.1 source-interface ethernet 2/1`	Configures a host receiver for SNMPv2c traps or informs. The *ip-address* can be an IPv4 address. Use **?** to determine the supported interface types. The UDP port number range is from 0 to 65535. This configuration overrides the global source interface configuration.

Use the following command in global configuration mode to configure a source interface for sending out all SNMP notifications:

Command	Purpose
snmp-server source-interface {traps | informs} *if-type if-number* **Example:** `router(config)# snmp-server source-interface traps ethernet 2/1`	Configures a source interface for sending out SNMPv2c traps or informs. Use **?** to determine the supported interface types.

Use the **show snmp source-interface** command to display information about configured source interfaces.

Configuring the Notification Target User

You must configure a notification target user on the device to send SNMPv3 inform notifications to a notification host receiver.

Cisco CG-OS uses the credentials of the notification target user to encrypt the SNMPv3 inform notification messages to the configured notification host receiver.

Note For authenticating and decrypting the received inform PDU, the notification host receiver should have the same user credentials as configured in Cisco CG-OS to authenticate and decrypt the informs.

Use the following command in global configuration mode to configure the notification target user:

Command	Purpose
snmp-server user name [auth {md5 | sha} *passphrase* **[auto] [priv [aes-128]** *passphrase*] [*engineID id*] **Example:** `router(config)# snmp-server user NMS auth sha abcd1234 priv abcdefgh engineID 00:00:00:63:00:01:00:10:20:15:10:03`	Configures the notification target user with the specified engine ID for the notification host receiver. The engineID format is a 12-digit colon-separated decimal number.

Configuring SNMP to Send Traps Using an Inband Port

You can configure SNMP to send traps using an inband port. To do so, you must configure the source interface (at the global or host level) to send the traps.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Router enters global configuration mode.
Step 2	**snmp-server source-interface traps** *if-type if-number*	Globally configures a source interface for sending out SNMP traps. Use **?** to determine the supported interface types. You can configure the source interface at the global level or at a host level. When the source interface is configured globally, any new host configuration uses the global configuration to send the traps. **Note**: To configure a source interface at the host level, use this command: **snmp-server host** *ip-address* **source-interface** *if-type if-number*.
Step 3	**show snmp source-interface**	(Optional) Displays information about configured source interfaces.
Step 4	**snmp-server host** *ip-address* [**udp_port** *port*]	Configures SNMP to communicate with the host receiver. The *ip-address* can be an IPv4 address. The UDP port number range is from 0 to 65535.

	Command	Purpose
Step 5	**show snmp host**	(Optional) Displays information about configured SNMP hosts.
Step 6	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to configure SNMP to send traps using a globally configured inband port:

```
router# configure terminal
router(config)# snmp-server source-interface traps ethernet 1/2
router(config)# show snmp source-interface
------------------------------------------------------------------------
Notification                    source-interface
------------------------------------------------------------------------
trap                            Ethernet1/2

inform                                -
------------------------------------------------------------------------

router(config)# snmp-server host 171.71.48.164
router(config)# show snmp host
------------------------------------------------------------------------
Host                            Port Version  Level  Type   SecName
------------------------------------------------------------------------
171.71.48.164                    162  v2c      noauth trap   public


Source interface: Ethernet 1/2
------------------------------------------------------------------------
```

Enabling SNMP Notifications

You can enable or disable notifications. If you do not specify a notification name, Cisco CG-OS enables all notifications.

Table 3-3 lists the commands that enable the notifications for Cisco CG-OS MIBs.

Note The **snmp-server enable traps** command enables both traps and informs, depending on the configured notification host receivers.

Table 3-3 Enabling SNMP Notifications

MIB	Related Commands
All notifications	**snmp-server enable traps**
CISCO-AAA-SERVER-MIB	**snmp-server enable traps aaa** **snmp-server enable traps aaa server-state-change**
CISCO-CALLHOME-MIB	**snmp-server enable traps callhome** **snmp-server enable traps callhome event-notify** **snmp-server enable traps callhome smtp-send-fail**
ENTITY-MIB, CISCO-ENTITY-SENSOR-MIB	**snmp-server enable traps entity** **snmp-server enable traps entity fru** **snmp-server enable traps entity entity_sensor** **snmp-server enable traps entity entity_mib_change** **snmp-server enable traps entity entity_module_status_change** **snmp-server enable traps entity entity_power_status_change** **snmp-server enable traps entity entity_module_inserted** **snmp-server enable traps entity entity_module_removed** **snmp-server enable traps entity entity_unrecognised_module** **snmp-server enable traps entity entity_fan_status_change** **snmp-server enable traps entity entity_power_out_change**
IF-MIB	**snmp-server enable traps link** **snmp-server enable traps link linkDown** **snmp-server enable traps link linkUp**
SNMPv2-MIB	**snmp-server enable traps snmp** **snmp-server enable traps snmp authentication**
CISCO-FEATURE-CONTROL-MIB	**snmp-server enable traps feature-control** **snmp-server enable traps feature-control FeatureOpStatusChange**
CISCO-SYSTEM-EXT-MIB	**snmp-server enable traps sysmgr** **snmp-server enable traps sysmgr cseFailSwCoreNotifyExtended**
ITRON-PRISM-C1222-MIB	**snmp-server enable traps c1222r** **snmp-server enable traps c1222r comm_module_idle_too_long** **snmp-server enable traps c1222r comm_module_enable_change**

Use the following commands in global configuration mode to enable the specified notification.

Command	Purpose
snmp-server enable traps **Example:** `router(config)# snmp-server enable traps`	Enables all SNMP notifications.
snmp-server enable traps aaa [**server-state-change**] **Example:** `router(config)# snmp-server enable traps aaa`	Enables the AAA SNMP notifications.
snmp-server enable traps callhome [event-notify] [smtp-send-fail] **Example:** `router(config)# snmp-server enable traps callhome`	Enables the CISCO-CALLHOME-MIB SNMP notifications. Optionally, enables the following specific notifications: • **event-notify**—Enables Call Home external event notifications. • **smtp-send-fail**—Enables SMTP message send fail notifications.
snmp-server enable traps entity [fru] **Example:** `router(config)# snmp-server enable traps entity`	Enables the ENTITY-MIB SNMP notifications.

Disabling LinkUp/LinkDown Notifications on an Interface

You can disable linkUp and linkDown notifications on an individual interface. You can use these limit notifications on a flapping interface (an interface that transitions between up and down repeatedly).

Use the following command in interface configuration mode to disable linkUp/linkDown notifications for the interface:

Command	Purpose
no snmp trap link-status **Example:** `router(config-if)# no snmp trap link-status`	Disables SNMP link-state traps for the interface. This command is enabled by default.

Displaying SNMP ifIndex for an Interface

The SNMP ifIndex is used across multiple SNMP MIBs to link related interface information. The ifIndex is also used by NetFlow to collect information on an interface.

Use the following command in any mode to display the SNMP ifIndex values for interfaces:

Command	Purpose
show interface snmp-ifindex **Example:** `router# show interface snmp-ifindex | grep -i Eth 2/1`	Displays the persistent SNMP ifIndex value from IF-MIB for all interfaces. Optionally, use the | keyword and the grep keyword to search for a particular interface in the output.

Enabling a One-time Authentication for SNMP over TCP

You can enable a one-time authentication for SNMP over a TCP session.

Use the following command in global configuration mode to enable a one-time authentication for SNMP over TCP:

Command	Purpose
snmp-server tcp-session [auth] **Example:** `router(config)# snmp-server tcp-session`	Enables a one-time authentication for SNMP over a TCP session. The default is disabled.

Assigning the SNMP Device Contact and Location Information

You can assign the device contact information, which is limited to 32 characters (without spaces) and the device location.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Router enters global configuration mode.
Step 2	**snmp-server contact** *name*	Configures sysContact, which is the SNMP contact name.
Step 3	**snmp-server location** *name*	Configures sysLocation, which is the SNMP location.
Step 4	**show snmp**	(Optional) Displays information about one or more destination profiles.
Step 5	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to configure the SNMP contact and location information:

```
router# configure terminal
router(config)# snmp-server contact Admin
router(config)# snmp-server location Lab-7
router(config)# copy running-config startup-config
```

Configuring the Context to Network Entity Mapping

You can configure an SNMP context to map to a logical network entity, such as a protocol instance.

BEFORE YOU BEGIN

Determine the logical network entity instance.

DETAILED STEPS

	Command	Purpose
Step 1	**configure terminal**	Router enters global configuration mode.
Step 2	**snmp-server context** *context-name* **[instance** *instance-name*]**[topology** *topology-name*]	Maps an SNMP context to a protocol instance or topology. The names can be any alphanumeric string up to 32 characters.
Step 3	**snmp-server mib community-map** *community-name* **context** *context-name*	(Optional) Maps an SNMPv2c community to an SNMP context. The names can be any alphanumeric string up to 32 characters.
Step 4	**show snmp context**	(Optional) Displays information about one or more SNMP contexts.
Step 5	**copy running-config startup-config**	(Optional) Saves this configuration change.

EXAMPLE

This example shows how to map OSPF instance Enterprise to the same SNMPv2c public community string.

```
router# configure terminal
router(config)# feature ospf
router(config)# router ospf Enterprise
router(config-router)# exit
router(config)# snmp-server context public1 instance Enterprise
router(config)# snmp-server mib community-map public context public1
router(config)# copy running-config startup-config
```

This example shows how to delete the mapping between an SNMP context and a logical network entity when operating in the global configuration mode.

```
router(config)# no snmp-server context public1
```

Note When deleting a context mapping (see example above), you only enter the context name in the **no snmp-server context** *context-name* command. You do not enter the instance or topology keywords and variable names as you did when configuring the item (see Step 2. If you use the **instance** or **topology** keywords when deleting the context mapping, then you configure a mapping between the context and a zero-length string

Disabling SNMP

You can disable SNMP on a device.

Use the following command in global configuration mode to disable SNMP:

Command	Purpose
no snmp-server protocol enable **Example:** `router(config)# no snmp-server protocol enable`	Disables SNMP. This command is enabled by default.

Modifying the AAA Synchronization Time

You can modify how long Cisco CG-OS holds the synchronized user configuration.

Use the following command in global configuration mode to modify the AAA synchronization time:

Command	Purpose
snmp-server aaa-user cache-timeout *seconds* **Example:** `router(config)# snmp-server aaa-user cache-timeout 1200`	Configures how long the AAA synchronized user configuration stays in the local cache. The range is from 1 to 86400 seconds. The default is 3600.

Verifying Configuration

To display the SNMP configuration information, perform one of the following tasks.

Command	Purpose
show interface snmp-ifidex	Displays the SNMP ifIndex value for all interfaces (from IF-MIB).
show running-config snmp [**all**]	Displays the SNMP running configuration.
show snmp	Displays the SNMP status.
show snmp community	Displays the SNMP community strings.
show snmp context	Displays the SNMP context mapping.
show snmp engineID	Displays the SNMP engineID.
show snmp group	Displays SNMP roles.
show snmp host	Displays information about configured SNMP hosts.
show snmp session	Displays SNMP sessions.
show snmp source-interface	Displays information about configured source interfaces.
show snmp trap	Displays the SNMP notifications enabled or disabled.
show snmp user	Displays SNMPv3 users.

Configuration Examples

This example shows how to configure Cisco CG-OS to send the Cisco linkUp or Down notifications to one notification host receiver and defines two SNMP users, Admin and NMS.

```
router# configure terminal
router(config)# snmp-server contact Admin@company.com
router(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh
router(config)# snmp-server user NMS auth sha abcd1234 priv abcdefgh engine ID
                00:00:00:63:00:01:00:22:32:15:10:03
router(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS
router(config)# snmp-server enable traps link cisco
```

This example shows how to configure SNMP to send traps using an inband port configured at the host level.

```
router# config t
router(config)# snmp-server host 171.71.48.164 version 2c public
router(config)# snmp-server host 171.71.48.164 source-interface ethernet 1/2
router(config)# show snmp host
-----------------------------------------------------------------------
Host                            Port Version  Level  Type   SecName
-----------------------------------------------------------------------
171.71.48.164                    162  v2c      noauth trap   public

Source interface: Ethernet 1/2
-----------------------------------------------------------------------

router(config)# snmp-server host 171.71.48.164
router(config)# show snmp host
-----------------------------------------------------------------------
Host                            Port Version  Level  Type   SecName
-----------------------------------------------------------------------
171.71.48.164                    162  v2c      noauth trap   public

Source interface: Ethernet 1/2
-----------------------------------------------------------------------
```

Useful Common MIBs

MIBs	MIBs Link
• SNMP-COMMUNITY-MIB • SNMP-FRAMEWORK-MIB • SNMP-NOTIFICATION-MIB • SNMP-TARGET-MIB • SNMPv2-MIB	To locate and download these MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml Click **SNMPv2 MIBs** to download these MIBs.

Feature History

Table 3-4 Feature History for SNMP

Feature Name	Release	Feature Information
SNMP	Cisco CG-OS Release CG2(1)	Initial support of the feature on the CGR 1000 Series Routers.