CHAPTER 1

Configuring SNMP

This chapter describes how to configure the SNMP feature in Cisco Nexus 5000 Series of switches.

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:

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. The Cisco Nexus 5000 Series switch 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 34180.

Note Cisco NX-OS does not support SNMP sets for Ethernet MIBs.

Cisco Nexus 5000 Series switch supports SNMPv1, SNMPv2c and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security.

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 connection to a neighbor router, or other significant events.

Cisco Nexus 5000 Series switch generates SNMP notifications as either traps or informs. Traps are less reliable than informs because the SNMP manager does not send any acknowledgment when it receives a trap. Cisco Nexus 5000 Series switch 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 Cisco Nexus 5000 Series switch never receives a response, it can send the inform request again.

You can configure the Cisco Nexus 5000 Series switch to send notifications to multiple host receivers. See the "Configuring SNMP Notification Receivers" section on page 1-7 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 the following:

- Message integrity—Ensures that a packet has not been tampered with in-transit.
- Authentication—Determines 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 contains the following topics:

Security Models and Levels for SNMPv1, v2, 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: SNMPv1, SNMPv2c, and SNMPv3. The security model combined with the security level determine the security mechanism applied when the SNMP message is processed.

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

User-Based Security Model

Table 1-1 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	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 AES-128	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. By default, the switch provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard. The switch also provides an option to use a 128-bit AES algorithm for privacy.

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.

Cisco Nexus 5000 Series uses two authentication protocols for SNMPv3:

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

Cisco Nexus 5000 Series 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 along with the **aes-128** token indicates 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 characters. If you use the localized key, you can specify a maximum of 130 characters.

Note For an SNMPv3 operation using the external AAA server, you must use AES for the privacy protocol in 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 Nexus 5000 Series 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 switch.

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

Cisco Nexus 5000 Series synchronizes user configuration in the following ways:

- The **auth** passphrase specified in the **snmp-server user** command becomes the password for the CLI user.
- The password specified in the **username** command becomes as the **auth** and **priv** passphrases for the SNMP user.
- Deleting a user using either SNMP or the CLI results in the user being deleted for both SNMP and the CLI.
- User-role mapping changes are synchronized in SNMP and the CLI.

Note When you configure passphrase/password in localized key/encrypted format, Cisco Nexus 5000 Series does not synchronize the password.

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 three accesses: read access, write access, and notification access. Each access can be enabled or disabled within each group.

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

Configuration Guidelines and Limitations

SNMP has the following configuration guidelines and limitations:

- Cisco NX-OS supports read-only access to Ethernet MIBs.

Configuring SNMP

This section includes the following topics:

Note If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

Configuring SNMP Users

To configure a user for SNMP, perform this task:

	Command	Purpose
Step 1	`switch# configuration terminal`	Enters configuration mode.
Step 2	`switch(config)# 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.
Step 3	`switch(config-callhome)# show snmp user`	(Optional) Displays information about one or more SNMP users.
Step 4	`switch(config)# copy running-config startup-config`	(Optional) Saves this configuration change.

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 Nexus 5000 Series responds with an authorization Error for any SNMPv3 PDU request using securityLevel parameter of either noAuthNoPriv or authNoPriv.

To enforce SNMP message encryption for a user in the global configuration mode, perform this task:

Command	Purpose
`switch(config)# snmp-server user name enforcePriv`	Enforces SNMP message encryption for this user.

To enforce SNMP message encryption for all users in the global configuration mode, perform this task:

Command	Purpose
`switch(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.

To assign a role to an SNMP user in a global configuration mode, perform this task:

Command	Purpose
`switch(config)# snmp-server user name group`	Associates this SNMP user with the configured user role.

Creating SNMP Communities

You can create SNMP communities for SNMPv1 or SNMPv2c.

Tocreate an SNMP community string in a global configuration mode, perform this task:

Command	Purpose
`switch(config)# snmp-server community name group {ro | rw}`	Creates an SNMP community string.

Configuring SNMP Notification Receivers

You can configure Cisco Nexus 5000 Series to generate SNMP notifications to multiple host receivers.

To configure a host receiver for SNMPv1 traps in a global configuration mode, perform this task:

Command	Purpose
`switch(config)# snmp-server host ip-address traps {version 1] community [udp_port number]`	Configures a host receiver for SNMPv1 traps. The community can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

To configure a host receiver for SNMPv2c traps or informs in a global configuration mode, perform this task:

Command	Purpose
`switch(config)# snmp-server host ip-address {traps | informs} version 2c community [udp_port number]`	Configures a host receiver for SNMPv2c traps or informs. The community can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

To configure a host receiver for SNMPv3 traps or informs in a global configuration mode, perform this task:

Command	Purpose
`switch(config)# snmp-server host` *ip-address* {**traps** | **informs**} **version 3** {**auth** | **noauth** | **priv** } *username* [**udp_port** *number*]	Configures a host receiver for SNMPv2c traps or informs. The username can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

The following example shows how toconfigure a host receiver for an SNMPv3 inform:

```
switch(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS
```

Note The SNMP manager must know the user credentials (authKey/PrivKey) based on the SNMP engineID of the Cisco Nexus 5000 Series device to authenticate and decrypt the SNMPv3 messages.

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.

The Cisco Nexus 5000 Series switch 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 the Cisco Nexus 5000 Series switch to authenticate and decrypt the informs.

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

Command	Purpose
`switch(config)#` **snmp-server user** *name* [**auth** {md5 | sha} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*]	Configures the notification target user with the specified engine ID for notification host receiver. The engineID format is a 12-digit colon-separated hexadecimal number.

The following example shows how to configure a notification target user:

```
switch(config)# snmp-server user NMS auth sha abcd1234 priv abcdefgh enginID
00:00:00:63:00:01:00:a1:ac:15:10:03
```

Enabling SNMP Notifications

You can enable or disable notifications. If you do not specify a notification name, Cisco Nexus 5000 Series enables all notifications.

Table 1-2 lists the CLI commands that enable the notifications for Cisco Nexus 5000 Series MIBs.

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

Table 1-2 Enabling SNMP Notifications

MIB	Related Commands
All notifications	**snmp-server enable traps**
CISCO-AAA-SERVER-MIB	**snmp-server enable traps aaa**
ENITY-MIB, CISCO-ENTITY-FRU-CONTROL-MIB, CISCO-ENTITY-SENSOR-MIB	**snmp-server enable traps entity** **snmp-server enable traps entity fru**
CISCO-LICENSE-MGR-MIB	**snmp-server enable traps license**
IF-MIB	**snmp-server enable traps link**
CISCO-PSM-MIB	**snmp-server enable traps port-security**
SNMPv2-MIB	**snmp-server enable traps snmp** **snmp-server enable traps snmp authentication**
CISCO-FCC-MIB	**snmp-server enable traps fcc**
CISCO-DM-MIB	**snmp-server enable traps fcdomain**
CISCO-NS-MIB	**snmp-server enable traps fcns**
CISCO-FCS-MIB	**snmp-server enable traps fcs discovery-complete** **snmp-server enable traps fcs request-reject**
CISCO-FDMI-MIB	**snmp-server enable traps fdmi**
CISCO-FSPF-MIB	**snmp-server enable traps fspf**
CISCO-PSM-MIB	**snmp-server enable traps port-security**
CISCO-RSCN-MIB	**snmp-server enable traps rscn** **snmp-server enable traps rscn els** **snmp-server enable traps rscn ils**
CISCO-ZS-MIB	**snmp-server enable traps zone** **snmp-server enable traps zone default-zone-behavior-change** **snmp-server enable traps zone merge-failure** **snmp-server enable traps zone merge-success** **snmp-server enable traps zone request-reject** **snmp-server enable traps zone unsupp-mem**

Note The license notifications are enabled by default. All other notifications are disabled by default.

To enable the specified notification in the global configuration mode, perform one of the following tasks:

Command	Purpose
`switch(config)# snmp-server enable traps`	Enables all SNMP notifications.
`switch(config)# snmp-server enable traps aaa [server-state-change]`	Enables the AAA SNMP notifications.
`switch(config)# snmp-server enable traps entity [fru]`	Enables the ENTITY-MIB SNMP notifications.
`switch(config)# snmp-server enable traps license`	Enables the license SNMP notification.
`switch(config)# snmp-server enable traps port-security`	Enables the port security SNMP notifications.
`switch(config)# snmp-server enable traps snmp [authentication]`	Enables the SNMP agent notifications.

Configuring linkUp/linkDown Notifications

You can configure which linkUp/linkDown notifications to enable on a device. You can enable the following types of linkUp/linkDown notifications:

- Cisco—Cisco Nexus 5000 Series sends only the Cisco-defined notifications (cieLinkUp, cieLinkDow in CISCO-IF-EXTENSION-MIB.my), if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface.
- IETF—Cisco Nexus 5000 Series sends only the IETF-defined notifications (linkUp, linkDown in IF-MIB) with only the defined varbinds, if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface.
- IEFT extended—Cisco Nexus 5000 Series sends only the IETF-defined notifications (linkUp, linkDown defined in IF-MIB), if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface. Cisco Nexus 5000 Series adds additional varbinds specific to Cisco Systems in addition to the varbinds defined in the IF-MIB. This is the default setting.
- IEFT Cisco—Cisco Nexus 5000 Series sends the notifications (linkUp, linkDown) defined in IF-MIB and notifications (cieLinkUp, cieLinkDown) defined in CISCO-IF-EXTENSION-MIB.my , if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface. Cisco Nexus 5000 Series sends only the varbinds defined in the linkUp and linkDown notifications.
- IEFT extended Cisco—Cisco Nexus 5000 Series sends the notifications (linkUp, linkDown) defined in IF-MIB and notifications (cieLinkUp, cieLinkDown) defined in CISCO-IF-EXTENSION-MIB.my, if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface. Cisco Nexus 5000 Series adds additional varbinds specific to Cisco Systems in addition to the varbinds defined in the IF-MIB for the linkUp and linkDown notifications.

To configure the type of linkUp/linkDown notifications in a global configuration mode, perform this task:

Command	Purpose
`switch(config)# snmp-server enable traps link [cisco] [ietf | ietf-extended]`	Enables the link SNMP notifications.

Disabling Up/ Down Notifications on an Interface

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

To disable linkUp/linkDown notifications for the interface in interface configuration mode, perform this task:

Command	Purpose
`switch(config-if)# no snmp trap link-status`	Disables SNMP link-state traps for the interface. Enabled by default.

Enabling One-Time Authentication for SNMP over TCP

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

To enable one-time authentication for SNMP over TCP in global configuration mode, perform this task:

Command	Purpose
`switch(config)# snmp-server tcp-session [auth]`	Enables a one-time authentication for SNMP over a TCP session. Default is disabled.

Assigning SNMP Switch Contact and Location Information

You can assign the switch contact information, which is limited to 32 characters (without spaces) and the switch location. To assign the information, perform this task:

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

Verifying SNMP Configuration

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

Command	Purpose
`show snmp`	Displays the SNMP status.
`show snmp community`	Displays the SNMP community strings.
`show snmp engineID`	Displays the SNMP engineID.
`show snmp group`	Displays SNMP roles.
`show snmp sessions`	Displays SNMP sessions.
`show snmp trap`	Displays the SNMP notifications enabled or disabled.
`show snmp user`	Displays SNMPv3 users.

SNMP Example Configuration

This example configures Cisco Nexus 5000 Series to send the Cisco linkUp/linkDown notifications to one notification host receiver and defines two SNMP users, Admin and NMS:

```
configuration terminal
 snmp-server contact Admin@company.com
 snmp-server user Admin auth sha abcd1234 priv abcdefgh
 snmp-server user NMS auth sha abcd1234 priv abcdefgh enginID
00:00:00:63:00:01:00:a1:ac:15:10:03
 snmp-server host 192.0.2.1 informs version 3 auth NMS
 snmp-server host 192.0.2.1
 snmp-server enable traps link cisco
```

Default Settings

Table 1-3 lists the default settings for SNMP parameters.

Table 1-3 Default SNMP Parameters

Parameters	Default
license notifications	enabled
linkUp/Down notification type	ietf-extended