CHAPTER 10

Configuring SNMP

This chapter describes how to configure the SNMP including users, message encryption, notifications, authentication over TCP, and so forth.

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. Cisco Nexus 1000V 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.

Note SNMP Role Based Access Control (RBAC) is not supported.

SNMPv1, SNMPv2c, and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security are supported.

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.

SNMP notifications are generated 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 Nexus 1000V 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 Nexus 1000V never receives a response, it can send the inform request again.

You can configure Cisco Nexus 1000V to send notifications to multiple host receivers. See the "Configuring SNMP Notification Receivers" section on page 10-8 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 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 includes 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 10-1 identifies what the combinations of security models and levels mean.

Table 10-1 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	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

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 Nexus 1000V uses two authentication protocols for SNMPv3:

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

Cisco Nexus 1000V 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 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 Nexus 1000V 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 1000V 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 as the authentication and privacy passphrases for the SNMP user.
- If you delete a user using either SNMP or the CLI, the user is 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 passphrase/password in localized key/encrypted format, Cisco Nexus 1000V does not synchronize the password.

Cisco NX-OS holds the synchronized user configuration for 60 minutes by default. See the "Modifying the AAA Synchronization Time" section on page 10-13 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.

High Availability

Stateless restarts for SNMP are supported. After a reboot or supervisor switchover, the running configuration is applied.

Guidelines and Limitations

SNMP has the following configuration guidelines and limitations:

- Read-only access to some SNMP MIBs is supported. See the Cisco NX-OS MIB support list at the following URL for more information:

  http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml
- SNMP Role Based Access Control (RBAC) is not supported.
- The SNMP set command is supported by the following Cisco MIBs:
  - CISCO-IMAGE-UPGRADE-MIB
  - CISCO-CONFIG-COPY-MIB
- The recommended SNMP polling interval time is 5 minutes.

Default Settings

Table 10-2 lists the default settings for SNMP parameters.

Table 10-2 Default SNMP Parameters

Parameters	Default
license notifications	enabled

Configuring SNMP

This section includes the following topics:

- Configuring SNMP Users, page 10-6

Note Be aware that the Cisco NX-OS commands for this feature may differ from those used in Cisco IOS.

Configuring SNMP Users

Use this procedure to configure a user for SNMP.

BEFORE YOU BEGIN

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **config t**
2. **snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*] [**localizedkey**]]
3. **show snmp user**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** switch# config t Enter configuration commands, one per line. End with CNTL/Z. switch(config)#	Enters global configuration mode.
Step 2	**snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*] [**localizedkey**]] **Example:** switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh	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 **localizekey** keyword, the passphrase an 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** **Example:** switch(config-callhome)# show snmp user	(Optional) Displays information about one or more SNMP users.
Step 4	**copy running-config startup-config** **Example:** switch(config)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

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

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh
```

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 1000V 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:** switch(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:** `switch(config)# snmp-server globalEnforcePriv`	Enforces SNMP message encryption for all users.

Creating SNMP Communities

You can create SNMP communities for SNMPv1 or SNMPv2c.

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

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

Configuring SNMP Notification Receivers

You can configure Cisco Nexus 1000V to generate SNMP notifications to multiple host receivers.

Use the following command in global configuration mode to configure a host receiver for SNMPv1 traps:

Command	Purpose
snmp-server host *ip-address* **traps version 1** *community* [**udp_port** *number*] **Example:** `switch(config)# snmp-server host 192.0.2.1 traps version 1 public`	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.

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:** `switch(config)# snmp-server host 192.0.2.1 informs version 2c public`	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.

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*] **Example:** `switch(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS`	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.

Note The SNMP manager must know the user credentials (authKey/PrivKey) based on the SNMP engine ID of the Cisco Nexus 1000V 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.

Cisco Nexus 1000V 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 Nexus 1000V to authenticate and decrypt the inform s.

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:** `switch(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 notification host receiver. The engineID format is a 12-digit colon-separated decimal number.

Enabling SNMP Notifications

You can enable or disable notifications. If you do not specify a notification name, Cisco Nexus 1000V enables all notifications.

Table 10-3 lists the commands that enable the notifications for Cisco Nexus 1000V MIBs.

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

Table 10-3 Enabling SNMP Notifications

MIB	Related Commands
All notifications	**snmp-server enable traps**
CISCO-AAA-SERVER-MIB	**snmp-server enable traps aaa**
ENITY-MIB	**snmp-server enable traps entity**
CISCO-ENTITY-FRU-CONTROL-MIB	**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**

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

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

Command	Purpose
snmp-server enable traps **Example:** `switch(config)# snmp-server enable traps`	Enables all SNMP notifications.
snmp-server enable traps aaa [**server-state-change**] **Example:** `switch(config)# snmp-server enable traps aaa`	Enables the AAA SNMP notifications.
snmp-server enable traps entity [**fru**] **Example:** `switch(config)# snmp-server enable traps entity`	Enables the ENTITY-MIB SNMP notifications.
snmp-server enable traps license **Example:** `switch(config)# snmp-server enable traps license`	Enables the license SNMP notification.
snmp-server enable traps link **Example:** `switch(config)# snmp-server enable traps link`	Enables the link SNMP notifications.

Command	Purpose
snmp-server enable traps port-security **Example:** `switch(config)# snmp-server enable traps port-security`	Enables the port security SNMP notifications.
snmp-server enable traps snmp [**authentication**] **Example:** `switch(config)# snmp-server enable traps snmp`	Enables the SNMP agent notifications.

Disabling LinkUp/LinkDown 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).

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

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

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 one-time authentication for SNMP over TCP:

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

Assigning the 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.

BEFORE YOU BEGIN

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **config t**
2. **snmp-server contact** *name*
3. **snmp-server location** *name*
4. **show snmp**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`switch# config t`
	`Enter configuration commands, one per line. End with CNTL/Z.`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**snmp-server contact** *name* **Example:** `switch(config)# snmp-server contact Admin`	Configures sysContact, which is the SNMP contact name.
Step 3	**snmp-server location** *name* **Example:** `switch(config)# snmp-server location Lab-7`	Configures sysLocation, which is the SNMP location.
Step 4	**show snmp** **Example:** `switch(config)# show snmp`	(Optional) Displays information about one or more destination profiles.
Step 5	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

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

```
switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# snmp contact Admin
switch(config)# snmp location Lab-7
```

Disabling SNMP

You can disable the SNMP protocol on a device.

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

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

Modifying the AAA Synchronization Time

You can modify how long Cisco NX-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:** `switch(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 the SNMP Configuration

To display the SNMP configuration, use the following commands:

Command	Purpose
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 session	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 sending the Cisco linkUp/Down notifications to one notification host receiver using the Blue VRF and defines two SNMP users, Admin and NMS:

```
config t
 snmp-server contact Admin@company.com
 snmp-server user Admin auth sha abcd1234 priv abcdefgh
```

```
 snmp-server user NMS auth sha abcd1234 priv abcdefgh engineID
00:00:00:63:00:01:00:22:32:15:10:03
 snmp-server host 192.0.2.1 informs version 3 auth NMS
 snmp-server host 192.0.2.1 use-vrf Blue
 snmp-server enable traps link cisco
```

Additional References

For additional information related to implementing SNMP, see the following sections:

- Related Documents, page 10-14
- Standards, page 10-14
- MIBs, page 10-15

Related Documents

Related Topic	Document Title
Complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4a)*
MIBs	http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

Table 10-4 Supported MIBs

MIBs	MIBs Link
• CISCO-TC • SNMPv2-MIB • SNMP-COMMUNITY-MIB • SNMP-FRAMEWORK-MIB • SNMP-NOTIFICATION-MIB • SNMP-TARGET-MIB • ENTITY-MIB • IF-MIB • CISCO-ENTITY-EXT-MIB • CISCO-ENTITY-FRU-CONTROL-MIB • CISCO-FLASH-MIB • CISCO-IMAGE-MIB • CISCO-VIRTUAL-NIC-MIB • CISCO-ENTITY-VENDORTYPE-OID-MIB • NOTIFICATION-LOG-MIB • IANA-ADDRESS-FAMILY-NUMBERS-MIB • IANAifType-MIB • IANAiprouteprotocol-MIB • HCNUM-TC	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml
• CISCO-VLAN-MEMBERSHIP-MIB • CISCO-SYSTEM-MIB • CISCO-SYSTEM-EXT-MIB • CISCO-IMAGE-MIB • CISCO-IMAGE-UPGRADE-MIB • CISCO-BRIDGE-MIB • CISCO-CONFIG-COPY-MIB • CISCO-SYSLOG-EXT-MIB • CISCO-PROCESS-MIB • CISCO-AAA-SERVER-MIB • CISCO-AAA-SERVER-EXT-MIB • CISCO-COMMON-ROLES-MIB • CISCO-COMMON-MGMT-MIB	

Feature History for SNMP

This section provides the SNMP feature release history.

Feature Name	Releases	Feature Information
SNMP	4.0(4)SV1(1)	This feature was introduced.