



Configuring SNMP

This chapter describes how to configure the SNMP feature on Cisco NX-OS devices.

This chapter contains the following sections:

- [Finding Feature Information, on page 1](#)
- [About SNMP, on page 1](#)
- [Guidelines and Limitations for SNMP, on page 8](#)
- [Default Settings for SNMP, on page 8](#)
- [Configuring SNMP, on page 9](#)
- [Verifying SNMP Configuration, on page 33](#)
- [Configuration Examples for SNMP, on page 33](#)
- [Additional References, on page 35](#)
- [Feature History for SNMP, on page 36](#)

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at <https://tools.cisco.com/bugsearch/> and the release notes for your software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the "New and Changed Information" chapter or the Feature History table in this chapter.

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.

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 device 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.

The device supports SNMPv1, SNMPv2c, and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security.

Cisco NX-OS supports SNMP over IPv6.

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 NX-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. The device 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 device never receives a response, it can send the inform request again.

You can configure Cisco NX-OS to send notifications to multiple host receivers.

The following table lists the SNMP traps that are enabled by default.

Trap Type	Description
generic	: coldStart
generic	: warmStart
entity	: entity_mib_change
entity	: entity_module_status_change
entity	: entity_power_status_change
entity	: entity_module_inserted
entity	: entity_module_removed
entity	: entity_unrecognised_module
entity	: entity_fan_status_change
entity	: entity_power_out_change
link	: linkDown
link	: linkUp

Trap Type	Description
link	: extended-linkDown
link	: extended-linkUp
link	: cieLinkDown
link	: cieLinkUp
link	: delayed-link-state-change
rf	: redundancy_framework
license	: notify-license-expiry
license	: notify-no-license-for-feature
license	: notify-licensefile-missing
license	: notify-license-expiry-warning
upgrade	: UpgradeOpNotifyOnCompletion
upgrade	: UpgradeJobStatusNotify
rmon	: risingAlarm
rmon	: fallingAlarm
rmon	: hcRisingAlarm
rmon	: hcFallingAlarm
entity	: entity_sensor

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.

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. The following table identifies what the combinations of security models and levels mean.



Note noAuthnoPriv is not supported in SNMPv3.

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	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 NX-OS uses two authentication protocols for SNMPv3:

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

Cisco NX-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 using 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 NX-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 switch.

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

Cisco NX-OS synchronizes the 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 NX-OS does not synchronize the user information (passwords, roles, and so on).

Cisco NX-OS holds the synchronized user configuration for 60 minutes by default.

AAA Exclusive Behavior in SNMPv3 Servers

The AAA exclusive behavior feature enables you to authenticate users based on location.

A unique SNMPv3 user is not authenticated if the user is not a local user or a remote AAA user. If the user exists in both the local and remote database, the user will be authenticated or rejected based on whether AAA exclusive behavior is enabled or not.

Table 2: AAA Exclusive Behavior Scenarios

User Location	AAA Server	AAA Exclusive Behavior	User Authentication
Local user database	Disabled	Enabled	User is authenticated.
Local user database	Enabled	Enabled	User is not authenticated.
Local user database	Enabled	Disabled	User is authenticated.
Local user database	Disabled	Disabled	User is authenticated.
Remote and local user databases (same username)	Enabled	Enabled	Remote user is authenticated, but the local user is not authenticated. ¹
Remote and local user databases (same username)	Disabled	Enabled	Local user is authenticated, but the remote user is not authenticated.
Remote and local user databases (same username)	Disabled	Disabled	Local user is authenticated, but the remote user is not authenticated.
Remote and local user databases (same username)	Enabled	Disabled	Local user is authenticated, but the remote user is not authenticated.

¹ This works only when there is FM/DM concept from NMS server where it syncs user credentials automatically to the N7k switch which results in expected SNMP walk output. Otherwise, the user credentials will not sync to switch and should be done manually using hidden CLI on switch.



Note When AAA servers are unreachable, a fallback option can be configured on the server so that a user is validated against the local user database. The SNMPv3 server returns an error if the user is not available in the local database or in the remote user database. The SNMPv3 server returns an “Unknown user” message without checking the availability of AAA servers when a user is not available in the remote user database.

Group-Based SNMP Access



Note Because *group* is a standard SNMP term used industry-wide, we refer to roles as groups 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.

SNMP and Embedded Event Manager

The Embedded Event Manager (EEM) feature monitors events, including SNMP MIB objects, and triggers an action based on these events. One of the actions could be to send an SNMP notification. EEM sends the `cEventMgrPolicyEvent` of `CISCO-EMBEDDED-EVENT-MGR-MIB` as the SNMP notification.

Multiple Instance Support

A device can support multiple instances of a logical network entity, such as protocol instances or virtual routing and forwarding (VRF) instances. Most existing MIBs cannot distinguish between these multiple logical network entities. For example, the original OSPF-MIB assumes a single protocol instance on a device, but you can now configure multiple OSPF instances on a device.

SNMPv3 uses contexts to distinguish between these multiple instances. An SNMP context is a collection of management information that you can access through the SNMP agent. A device can support multiple contexts for different logical network entities. An SNMP context allows the SNMP manager to access one of the multiple instances of a MIB module supported on the device for the different logical network entities.

Cisco NX-OS supports the `CISCO-CONTEXT-MAPPING-MIB` to map between SNMP contexts and logical network entities. You can associate an SNMP context to a VRF, protocol instance, or topology.

SNMPv3 supports contexts with the `contextName` field of the SNMPv3 PDU. You can map this `contextName` field to a particular protocol instance or VRF.

For SNMPv2c, you can map the SNMP community to a context using the `snmpCommunityContextName` MIB object in the `SNMP-COMMUNITY-MIB` (RFC 3584). You can then map this `snmpCommunityContextName` to a particular protocol instance or VRF using the `CISCO-CONTEXT-MAPPING-MIB` or the CLI.

High Availability for SNMP

Cisco NX-OS supports stateless restarts for SNMP. After a reboot or supervisor switchover, Cisco NX-OS applies the running configuration.

Virtualization Support for SNMP

Cisco NX-OS supports one instance of the SNMP per virtual device context (VDC). By default, Cisco NX-OS places you in the default VDC. For more information, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*.

SNMP supports multiple MIB module instances and maps them to logical network entities. For more information, see the “Multiple Instance Support” section.

SNMP is also VRF aware. You can configure SNMP to use a particular VRF to reach the SNMP notification host receiver. You can also configure SNMP to filter notifications to an SNMP host receiver based on the VRF where the notification occurred. For more information, see the “Configuring SNMP Notification Receivers with VRFs” section.

Guidelines and Limitations for SNMP

SNMP has the following configuration guidelines and limitations:

- To clear snmp counters from an interface use the **clear counters interface all snmp** command, or this command can be applied per interface basis. This is done because there are different data structures for SNMP and CLI counters. This behavior is common across all Cisco Nexus platforms.
- Access control list (ACLs) can be applied only to local SNMPv3 users configured on the switch. ACLs cannot be applied to remote SNMPv3 users stored on Authentication, Authorization, and Accounting (AAA) servers.
- Cisco NX-OS supports read-only access to some SNMP MIBs. See the Cisco NX-OS MIB support list at the following URL for more information: <ftp://ftp.cisco.com/pub/mibs/supportlists/nexus7000/Nexus7000MIBSupportList.html>

Default Settings for SNMP

The following table lists the default settings for SNMP parameters.

Parameters	Default
License notifications	Enabled

Configuring SNMP



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



Note You can configure up to 10 SNMP hosts on a device.

Configuring SNMP Users

You can configure a user for SNMP.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	snmp-server user <i>name</i> [auth { md5 sha } <i>passphrase</i> [auto] [priv [aes-128] <i>passphrase</i>] [engineID <i>id</i>] [localizedkey]] Example: <pre>switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh</pre>	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	(Optional) show snmp user Example: <pre>switch(config) # show snmp user</pre>	Displays information about one or more SNMP users.
Step 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

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 NX-OS responds with an authorization error for any SNMPv3 PDU request using a security level parameter of either **noAuthNoPriv** or **authNoPriv**.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	snmp-server user <i>name</i> enforcePriv Example: switch(config)# snmp-server user Admin enforcePriv	Enforces SNMP message encryption for this user.
Step 3	snmp-server globalEnforcePriv Example: switch(config)# snmp-server globalEnforcePriv	Enforces SNMP message encryption for all users.
Step 4	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

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.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.

	Command or Action	Purpose
Step 2	snmp-server user <i>name group</i> Example: <pre>switch(config)# snmp-server user Admin superuser</pre>	Associates this SNMP user with the configured user role.
Step 3	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Creating SNMP Communities

You can create SNMP communities for SNMPv1 or SNMPv2c.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	snmp-server community <i>name {group group ro rw}</i> Example: <pre>switch(config)# snmp-server community public ro</pre>	Creates an SNMP community string.
Step 3	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Filtering SNMP Requests

You can assign an access control list (ACL) to an SNMPv3 user or SNMPv3 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)

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	snmp-server user name [use-ipv4acl ipv4acl-name] [use-ipv6acl ipv6acl-name] Example: <pre>switch(config)# snmp-server community public use-ipv4acl myacl</pre>	Assigns an IPv4 or IPv6 ACL to an SNMPv3 user to filter SNMP requests. Note The AAA server must support the creation of SNMPv3 users.
Step 3	snmp-server community name [use-ipv4acl ipv4acl-name] [use-ipv6acl ipv6acl-name] Example: <pre>switch(config)# snmp-server community public use-ipv4acl myacl</pre>	Assigns an IPv4 or IPv6 ACL to an SNMPv3 community to filter SNMP requests.
Step 4	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Authenticating SNMPv3 Users Based on Location

You can authenticate local or remote SNMPv3 users based on their location.

Use the following command in global configuration mode to enable AAA exclusive behavior in SNMPv3 servers:

Command	Purpose
snmp-server aaa exclusive-behavior enable	<p>Enables the AAA exclusive behavior in SNMPv3 servers to authenticate users based on location.</p> <p>Depending on the location of the user and whether the AAA server is enabled, the exclusive behavior is as follows:</p> <ul style="list-style-type: none"> • If the user is a local user and the AAA server is enabled, queries for the user will fail with an “Unknown user” message. • If the user is a remote AAA user and the AAA server is disabled, queries for the user will fail with an “Unknown user” message. • If the user is both a local user and a remote AAA user and the AAA server is enabled, the queries with remote credentials will succeed, and queries with local credentials will fail with an “Incorrect password” message. If the AAA server is disabled, queries with local remote credentials will succeed, and queries with remote credentials will fail with an “Incorrect password” message.

Configuring SNMP Notification Receivers

You can configure Cisco NX-OS to generate SNMP notifications to multiple host receivers.

Procedure

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example:</p> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	<p>snmp-server host <i>ip-address</i> traps version 1 community [udp_port number]</p> <p>Example:</p> <pre>switch(config)# snmp-server host 192.0.2.1 traps version 1 public</pre>	Configures a host receiver for SNMPv1 traps. The <i>ip-address</i> can be an IPv4 or IPv6 address. The <i>community</i> can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.
Step 3	<p>snmp-server host <i>ip-address</i> {traps informs} version 2c community [udp_port number]</p> <p>Example:</p> <pre>switch(config)# snmp-server host 192.0.2.1 informs version 2c public</pre>	Configures a host receiver for SNMPv2c traps or informs. The <i>ip-address</i> can be an IPv4 or IPv6 address. The <i>community</i> can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

	Command or Action	Purpose
Step 4	snmp-server host <i>ip-address</i> { traps informs } version 3 { auth noauth priv } <i>username</i> [udp_port <i>number</i>] Example: <pre>switch(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS</pre>	Configures a host receiver for SNMPv3 traps or informs. The <i>ip-address</i> can be an IPv4 or IPv6 address. The <i>username</i> 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 NX-OS device to authenticate and decrypt the SNMPv3 messages.
Step 5	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

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 a source interface 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.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	snmp-server host <i>ip-address</i> source-interface <i>if-type if-number</i> [udp_port <i>number</i>] Example: <pre>switch(config)# snmp-server host 192.0.2.1 source-interface ethernet 2/1</pre>	Configures a host receiver for SNMPv2c traps or informs. The <i>ip-address</i> can be an IPv4 or IPv6 address. Use ? to determine the supported interface types. The UDP port number range is from 0 to 65535.

	Command or Action	Purpose
		This configuration overrides the global source interface configuration.
Step 3	snmp-server source-interface {traps informs} <i>if-type if-number</i> Example: <pre>switch(config)# snmp-server source-interface traps ethernet 2/1</pre>	Configures a source interface for sending out SNMPv2c traps or informs. Use ? to determine the supported interface types.
Step 4	show snmp source-interface Example: <pre>switch(config)# show snmp source-interface</pre>	Displays 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 NX-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 NX-OS to authenticate and decrypt the informs.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	snmp-server user <i>name</i> [auth {md5 sha} <i>passphrase</i> [auto] [priv [aes-128] <i>passphrase</i>] [engineID <i>id</i>] Example: <pre>switch(config)# snmp-server user NMS auth sha abcd1234 priv abcdefgh engineID 00:00:00:63:00:01:00:10:20:15:10:03</pre>	Configures the notification target user with the specified engine ID for the notification host receiver. The engine ID format is a 12-digit colon-separated decimal number.
Step 3	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Configuring SNMP Notification Receivers with VRFs

SNMP adds entries into the cExtSnmptargetVrfTable of the CISCO-SNMP-TARGET-EXT-MIB when you configure the VRF reachability and filtering options for an SNMP notification receiver.



Note You must configure the host before configuring the VRF reachability or filtering options.

You can configure Cisco NX-OS to use a configured VRF to reach the host receiver or to filter notifications based on the VRF in which the notification occurred.

Procedure

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example:</p> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	<p>[no] snmp-server host ip-address use-vrf vrf-name [udp_port number]</p> <p>Example:</p> <pre>switch(config)# snmp-server host 192.0.2.1 use-vrf Blue</pre>	<p>Configures SNMP to use the selected VRF to communicate with the host receiver. The <i>ip-address</i> can be an IPv4 or IPv6 address. The VRF name can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535. This command adds an entry into the ExtSnmptargetVrfTable of the CISCO-SNMP-TARGET-EXT-MB.</p> <p>The no form of this command removes the VRF reachability information for the configured host and removes the entry from the ExtSnmptargetVrfTable of the CISCO-SNMP-TARGET-EXT-MB.</p> <p>Note This command does not remove the host configuration.</p>
Step 3	<p>[no] snmp-server host ip-address filter-vrf vrf-name [udp_port number]</p> <p>Example:</p> <pre>switch(config)# snmp-server host 192.0.2.1 filter-vrf Red</pre>	<p>Filters notifications to the notification host receiver based on the configured VRF. The <i>ip-address</i> can be an IPv4 or IPv6 address. The VRF name can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.</p> <p>This command adds an entry into the ExtSnmptargetVrfTable of the CISCO-SNMP-TARGET-EXT-MB.</p> <p>The no form of this command removes the VRF filter information for the configured host and removes the entry from the</p>

	Command or Action	Purpose
		ExtSnmptargetVrfTable of the CISCO-SNMP-TARGET-EXT-MB. Note This command does not remove the host configuration.
Step 4	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

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) and the VRF used to send the traps.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	snmp-server source-interface traps <i>if-type if-number</i> Example: switch(config)# snmp-server source-interface traps ethernet 1/2	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 the snmp-server host ip-address source-interface if-type if-number command.
Step 3	(Optional) show snmp source-interface Example: switch(config)# show snmp source-interface	Displays information about configured source interfaces.
Step 4	snmp-server host <i>ip-address use-vrf vrf-name [udp_port number]</i> Example:	Configures SNMP to use the selected VRF to communicate with the host receiver. The <i>ip-address</i> can be an IPv4 or IPv6 address. The VRF name can be any alphanumeric string up

	Command or Action	Purpose
	<pre>switch(config)# snmp-server host 171.71.48.164 use-vrf default</pre>	<p>to 255 characters. The UDP port number range is from 0 to 65535. This command adds an entry into the ExtSnmpTargetVrfTable of the CISCO-SNMP-TARGET-EXT-MB.</p> <p>Note By default, SNMP sends the traps using the management VRF. If you do not want to use the management VRF, you must use this command to specify the desired VRF.</p>
Step 5	<p>(Optional) show snmp host</p> <p>Example:</p> <pre>switch(config)# show snmp host</pre>	Displays information about configured SNMP hosts.
Step 6	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Enabling SNMP Notifications

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



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

The following table lists the commands that enable the notifications for Cisco NX-OS MIBs.

Table 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-BGP4-MIB	snmp-server enable traps bgp
CISCO-BGP-MIBv2	snmp-server enable traps bgp cbgp2

MIB	Related Commands
CISCO-STP-BRIDGE-MIB	snmp-server enable traps bridge snmp-server enable traps bridge newroot snmp-server enable traps bridge topologychange
CISCO-CALLHOME-MIB	snmp-server enable traps callhome snmp-server enable traps callhome event-notify snmp-server enable traps callhome smtp-send-fail
CISCO-CFS-MIB	snmp-server enable traps cfs snmp-server enable traps cfs merge-failure snmp-server enable traps cfs state-change-notif
CISCO-CONFIG-MAN-MIB	snmp-server enable traps config snmp-server enable traps config ccmCLIRunningConfigChanged
CISCO-EIGRP-MIB	snmp-server enable traps eigrp <i>[tag]</i>
ENTITY-MIB, CISCO-ENTITY-SENSOR-MIB	snmp-server enable traps entity snmp-server enable traps entity entity_fan_status_change snmp-server enable traps entity entity_mib_change snmp-server enable traps entity entity_module_inserted snmp-server enable traps entity entity_module_removed snmp-server enable traps entity entity_module_status_change snmp-server enable traps entity entity_power_out_change snmp-server enable traps entity entity_power_status_change snmp-server enable traps entity entity_unrecognised_module

MIB	Related Commands
CISCO-FEATURE-CONTROL-MIB	snmp-server enable traps feature-control snmp-server enable traps feature-control FeatureOpStatusChange
CISCO-HSRP-MIB	snmp-server enable traps hsrp snmp-server enable traps hsrp state-change
CISCO-LICENSE-MGR-MIB	snmp-server enable traps license snmp-server enable traps license notify-license-expiry snmp-server enable traps license notify-license-expiry-warning snmp-server enable traps license notify-licensefile-missing snmp-server enable traps license notify-no-license-for-feature
CISCO-INTERFACE-XCVR MONITOR-MIB	snmp-server enable traps link cisco-xcvr-mon-status-chg
IF-MIB	snmp-server enable traps link snmp-server enable traps link IETF-extended-linkDown snmp-server enable traps link IETF-extended-linkUp snmp-server enable traps link cisco-extended-linkDown snmp-server enable traps link cisco-extended-linkUp snmp-server enable traps link linkDown snmp-server enable traps link Up
OSPF-MIB, OSPF-TRAP-MIB	snmp-server enable traps ospf [tag] snmp-server enable traps ospf lsa snmp-server enable traps ospf rate-limit rate

MIB	Related Commands
CISCO-PORT-SECURITY-MIB	snmp-server enable traps port-security snmp-server enable traps port-security access-secure-mac-violation snmp-server enable traps port-security trunk-secure-mac-violation
CISCO-RF-MIB	snmp-server enable traps rf snmp-server enable traps rf redundancy_framework
CISCO-RMON-MIB	snmp-server enable traps rmon snmp-server enable traps rmon fallingAlarm snmp-server enable traps rmon hcFallingAlarm snmp-server enable traps rmon hcRisingAlarm snmp-server enable traps rmon risingAlarm
SNMPv2-MIB	snmp-server enable traps snmp snmp-server enable traps snmp authentication
CISCO-STPX-MIB	snmp-server enable traps stpx snmp-server enable traps stpx inconsistency snmp-server enable traps stpx loop-inconsistency snmp-server enable traps stpx root-inconsistency
CISCO-SYSTEM-EXT-MIB	snmp-server enable traps sysmgr snmp-server enable traps sysmgr cseFailSwCoreNotifyExtended

MIB	Related Commands
UPGRADE-MIB	snmp-server enable traps upgrade snmp-server enable traps upgrade UpgradeJobStatusNotify snmp-server enable traps upgrade UpgradeOpNotifyOnCompletion
ZONE-MIB	zone zone default-zone-behavior-changes zone merge-failure zone merge-success zone request-reject1 zone unsupp-mem

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

Command	Purpose
snmp-server enable traps	Enables all SNMP notifications.
snmp-server enable traps aaa [server-state-change]	Enables the AAA SNMP notifications. Optionally, enables the following specific notifications: <ul style="list-style-type: none"> • server-state-change—Enables AAA server state-change notifications.
snmp-server enable traps bgp [cbgp2]	Enables CISCO-BGP4-MIB SNMP notifications. Optionally, enables the following specific notifications: <ul style="list-style-type: none"> • bgp cbgp2—Enables CISCO-BGP4-MIBv2 SNMP notifications.
snmp-server enable traps bridge [newroot] [topologychange]	Enables STP bridge SNMP notifications. Optionally, enables the following specific notifications: <ul style="list-style-type: none"> • newroot—Enables STP new root bridge notifications. • topologychange—Enables STP bridge topology-change notifications.

Command	Purpose
snmp-server enable traps callhome [event-notify] [smtp-send-fail]	Enables Call Home notifications. Optionally, enables the following specific notifications: <ul style="list-style-type: none"> • event-notify—Enables Call Home external event notifications. • smtp-send-fail—Enables Simple Mail Transfer Protocol (SMTP) message send fail notifications.
snmp-server enable traps cfs [merge-failure] [state-change-notif]	Enables Cisco Fabric Services (CFS) notifications. Optionally, enables the following specific notifications: <ul style="list-style-type: none"> • merge-failure—Enables CFS merge-failure notifications. • state-change-notif—Enables CFS state-change notifications.
snmp-server enable traps config [ccmCLIRunningConfigChanged]	Enables SNMP notifications for configuration changes. <ul style="list-style-type: none"> • ccmCLIRunningConfigChanged—Enables SNMP notifications for configuration changes in the running or startup configuration.
snmp-server enable traps eigrp [tag]	Enables CISCO-EIGRP-MIB SNMP notifications.

Command	Purpose
<p>snmp-server enable traps entity [entity_fan_status_change] [entity_mib_change] [entity_module_inserted] [entity_module_removed] [entity_module_status_change] [entity_power_out_change] [entity_power_status_change] [entity_unrecognised_module]</p>	<p>Enables ENTITY-MIB SNMP notifications. Optionally, enables the following specific notifications:</p> <ul style="list-style-type: none"> • entity_fan_status_change—Enables entity fan status-change notifications. • entity_mib_change—Enables entity MIB change notifications. • entity_module_inserted—Enables entity module inserted notifications. • entity_module_removed—Enables entity module removed notifications. • entity_module_status_change—Enables entity module status-change notifications. • entity_power_out_change—Enables entity power-out change notifications. • entity_power_status_change—Enables entity power status-change notifications. • entity_unrecognised_module—Enables entity unrecognized module notifications.
<p>snmp-server enable traps feature-control [FeatureOpStatusChange]</p>	<p>Enables feature-control SNMP notifications. Optionally, enables the following specific notifications:</p> <ul style="list-style-type: none"> • FeatureOpStatusChange—Enables feature operation status-change notifications.
<p>snmp-server enable traps hsrp [state-change]</p>	<p>Enables CISCO-HSRP-MIB SNMP notifications. Optionally, enables the following specific notifications:</p> <ul style="list-style-type: none"> • state-change—Enables HSRP state-change notifications.

Command	Purpose
snmp-server enable traps license [notify-license-expiry] [notify-license-expiry-warning] [notify-licensefile-missing] [notify-no-license-for-feature]	Enables ENTITY-MIB SNMP notifications. Optionally, enables the following specific notifications: <ul style="list-style-type: none"> • notify-license-expiry—Enables license expiry notifications. • notify-license-expiry-warning—Enables license expiry warning notifications. • notify-licensefile-missing—Enables license file-missing notifications. • notify-no-license-for-feature—Enables no-license-installed-for-feature notifications.
snmp-server enable traps link [IETF-extended-linkDown] [IETF-extended-linkUp] [cisco-extended-linkDown] [cisco-extended-linkUp] [linkDown] [linkUp]	Enables IF-MIB link notifications. Optionally, enables the following specific notifications: <ul style="list-style-type: none"> • IETF-extended-linkDown—Enables Internet Engineering Task Force (IETF) extended link state down notifications. • IETF-extended-linkUp—Enables Internet Engineering Task Force (IETF) extended link state up notifications. • cisco-extended-linkDown—Enables Cisco extended link state down notifications. • cisco-extended-linkUp—Enables Cisco extended link state up notifications. • linkDown—Enables IETF link state down notifications. • linkUp—Enables IETF link state up notifications.
snmp-server enable traps ospf [tag] [lsa]	Enables Open Shortest Path First (OSPF) notifications. Optionally, enables the following specific notifications: <ul style="list-style-type: none"> • lsa—Enables OSPF link state advertisement (LSA) notifications.

Command	Purpose
<p>snmp-server enable traps port-security [access-secure-mac-violation] [trunk-secure-mac-violation]</p>	<p>Enables port-security SNMP notifications. Optionally, enables the following specific notifications:</p> <ul style="list-style-type: none"> • access-secure-mac-violation—Enables secure machine access control (MAC) violation notifications. • trunk-secure-mac-violation—Enables virtual LAN (VLAN) secure MAC violation notifications.
<p>snmp-server enable traps rf [redundancy-framework]</p>	<p>Enables redundancy framework (RF) SNMP notifications. Optionally, enables the following specific notifications:</p> <ul style="list-style-type: none"> • redundancy-framework—Enables RF supervisor switchover MIB notifications.
<p>snmp-server enable traps rmon [fallingAlarm] [hcFallingAlarm] [hcRisingAlarm] [risingAlarm]</p>	<p>Enables remote monitoring (RMON) SNMP notifications. Optionally, enables the following specific notifications:</p> <ul style="list-style-type: none"> • fallingAlarm—Enables RMON falling alarm notifications. • hcFallingAlarm—Enables RMON high-capacity falling alarm notifications. • hcRisingAlarm—Enables RMON high-capacity rising alarm notifications. • risingAlarm—Enables RMON rising alarm notifications.
<p>snmp-server enable traps snmp [authentication]</p>	<p>Enables general SNMP notifications. Optionally, enables the following specific notifications:</p> <ul style="list-style-type: none"> • authentication—Enables SNMP authentication notifications.

Command	Purpose
snmp-server enable traps stpx [inconsistency] [loop-inconsistency] [root-inconsistency]	Enables remote monitoring (RMON) SNMP notifications. Optionally, enables the following specific notifications: <ul style="list-style-type: none"> • inconsistency—Enables SNMP STPX MIB inconsistency update notifications. • loop-inconsistency—Enables SNMP STPX MIB loop-inconsistency update notifications. • root-inconsistency—Enables SNMP STPX MIB root-inconsistency update notifications.
snmp-server enable traps sysmgr [cseFailSwCoreNotifyExtended]	Enables software change notifications. Optionally, enables the following specific notifications: <ul style="list-style-type: none"> • cseFailSwCoreNotifyExtended—Enables software core notifications.
snmp-server enable traps upgrade [UpgradeJobStatusNotify] [UpgradeOpNotifyOnCompletion]	Enables upgrade notifications. Optionally, enables the following specific notifications: <ul style="list-style-type: none"> • UpgradeJobStatusNotify—Enables upgrade job status notifications. • UpgradeOpNotifyOnCompletion—Enables upgrade global status notifications.
snmp-server enable traps vtp [notifs] [vlancreate] [vlandelete]	Enables VTP notifications. Optionally, enables the following specific notifications: <ul style="list-style-type: none"> • notifs—Enables VTP notifications. • vlancreate—Enables VLAN creation notifications. • vlandelete—Enables VLAN deletion notifications.

Command	Purpose
snmp-server enable traps zone [default-zone-behavior-change] [merge-failure] [merge-success] [request-reject1] [unsupp-mem]	<p>Enables default zone change notifications. Optionally, enables the following specific notifications:</p> <ul style="list-style-type: none"> • default-zone-behavior-change—Enables default zone behavior change notifications. • merge-failure—Enables merge failure notifications. • merge-success—Enables merge success notifications. • request-reject1—Enables request reject notifications. • unsupp-mem—Enables unsupported member notifications.

Disabling Link 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).

Procedure

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example:</p> <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	<p>interface <i>type slot/port</i></p> <p>Example:</p> <pre>switch(config)# interface ethernet 2/2</pre>	Disables SNMP link-state traps for the interface. This command is enabled by default.
Step 3	<p>no snmp trap link-status</p> <p>Example:</p> <pre>switch(config-if)# no snmp trap link-status</pre>	Disables SNMP link-state traps for the interface. This command is enabled by default.
Step 4	<p>(Optional) copy running-config startup-config</p> <p>Example:</p> <pre>switch(config-if)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Displaying SNMP ifIndex for an Interface

The SNMP ifIndex is used across multiple SNMP MIBs to link related interface information.

Procedure

	Command or Action	Purpose
Step 1	show interface snmp-ifindex Example: <pre>switch# show interface snmp-ifindex grep -i Eth12/1 Eth12/1 441974784 (0x1a580000)</pre>	Displays the persistent SNMP ifIndex value from the 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.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	snmp-server tcp-session [auth] Example: <pre>switch(config)# snmp-server tcp-session</pre>	Enables a one-time authentication for SNMP over a TCP session. The default is disabled.
Step 3	(Optional) copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	Copies the running configuration to the startup configuration.

Assigning 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.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example:	Enters global configuration mode.

	Command or Action	Purpose
	switch# configure terminal switch(config)#	
Step 2	snmp-server contact <i>name</i> Example: switch(config)# snmp-server contact Admin	Configures sysContact, which is the SNMP contact name.
Step 3	snmp-server location <i>name</i> Example: switch(config)# snmp-server location Lab-7	Configures sysLocation, which is the SNMP location.
Step 4	(Optional) show snmp Example: switch(config)# show snmp	Displays information about one or more destination profiles.
Step 5	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

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 or VRF.

Before you begin

Determine the logical network entity instance. For more information on VRFs and protocol instances, see the *Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide* or the *Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide*.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	[no] snmp-server context <i>context-name</i> [instance <i>instance-name</i>] [vrf <i>vrf-name</i>] [topology <i>topology-name</i>] Example: switch(config)# snmp-server context public1 vrf red	Maps an SNMP context to a protocol instance, VRF, or topology. Before Release 6.2(2), the names can be any alphanumeric string up to 32 characters. In Release 6.2(2) and later releases, the string can include non alphanumeric characters. However, the best practice is to use alphanumeric characters only.

	Command or Action	Purpose
		The no option deletes the mapping between an SNMP context and a protocol instance, VRF, or topology. Note Do not enter an instance, VRF, or topology to delete a context mapping. If you use the instance, VRF, or topology keywords, you configure a mapping between the context and a zero-length string.
Step 3	(Optional) snmp-server mib community-map <i>community-name context context-name</i> Example: switch(config)# snmp-server mib community-map public context public1	Maps an SNMPv2c community to an SNMP context. The names can be any alphanumeric string up to 32 characters.
Step 4	(Optional) show snmp context Example: switch(config)# show snmp context	Displays information about one or more SNMP contexts.
Step 5	(Optional) copy running-config startup-config Example: switch(config)# copy running-config startup-config	Copies the running configuration to the startup configuration.

Disabling SNMP

You can disable SNMP on the device.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: switch# configure terminal switch(config)#	Enters global configuration mode.
Step 2	no snmp-server protocol enable Example: switch(config)# no snmp-server protocol enable	Disables SNMP. SNMP is enabled by default.

Managing the SNMP Server Counter Cache Update Timer

You can modify how long, in seconds Cisco NX-OS holds the cache port state.

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	snmp-server counter cache-timeout <i>seconds</i> Example: <pre>switch(config)# snmp-server counter cache-timeout 1800</pre>	Defines how long in seconds, the port states are held in the local cache. The counter cache is enabled by default, and the default cache timeout value is 10 seconds. When disabled, the default value for the SNMP cache expiry timeout is 140 seconds. The range is 1-3600. For end of row (EoR) switching - The range is from 10 to 3600.
Step 3	(Optional) show running-config snmp all Example: <pre>switch(config)# show running-config snmp all</pre>	Displays the configured SNMP-server counter cache update timeout value.
Step 4	no snmp-server counter cache enable Example: <pre>switch(config)# no snmp-server counter cache enable</pre>	Disables the counter cache update. When the counter cache update is disabled, the value set in the timeout parameter determines length of time the port states are held the counter cache.

Modifying the AAA Synchronization Time

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

Procedure

	Command or Action	Purpose
Step 1	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	Enters global configuration mode.
Step 2	snmp-server aaa-user cache-timeout <i>seconds</i> Example: <pre>switch(config)# snmp-server aaa-user cache-timeout 1200</pre>	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.
Step 3	(Optional) copy running-config startup-config Example:	Copies the running configuration to the startup configuration.

	Command or Action	Purpose
	switch(config)# copy running-config startup-config	

Verifying SNMP Configuration

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

Command	Purpose
show interface snmp-ifindex	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 for SNMP

This example shows how to configure Cisco NX-OS to send the Cisco linkUp or Down notifications to one notification host receiver using the Blue VRF and defines two SNMP users, Admin and NMS:

```
configure 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 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
```

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

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server host 171.71.48.164 version 2c public
switch(config)# snmp-server host 171.71.48.164 source-interface ethernet 1/2
switch(config)# show snmp host
-----
Host Port Version Level Type SecName
-----
171.71.48.164 162 v2c noauth trap public
Source interface: Ethernet 1/2
-----
switch(config)# snmp-server host 171.71.48.164 use-vrf default
switch(config)# show snmp host
-----
Host Port Version Level Type SecName
-----
171.71.48.164 162 v2c noauth trap public
Use VRF: default
Source interface: Ethernet 1/2
-----
```

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

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server source-interface traps ethernet 1/2
switch(config)# show snmp source-interface
-----
Notification source-interface
-----
trap Ethernet1/2
inform -
-----
switch(config)# snmp-server host 171.71.48.164 use_vrf default
switch(config)# show snmp host
-----
Host Port Version Level Type SecName
-----
171.71.48.164 162 v2c noauth trap public
Use VRF: default
Source interface: Ethernet 1/2
-----
```

This example shows how to map VRF red to the SNMPv2c public community string:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# vrf context red
switch(config-vrf)# exit
switch(config)# snmp-server context public1 vrf red
switch(config)# snmp-server mib community-map public context public1
```

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

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# feature ospf
```

```
switch(config)# router ospf Enterprise
switch(config-router)# exit
switch(config)# snmp-server context public1 instance Enterprise
switch(config)# snmp-server mib community-map public context public1
```

This example shows how to configure both IPv4 and IPv6 ACLs with the SNMPv3 “newstring” community:

```
switch# configure terminal
switch(config)# snmp-server community newstring use-ipv4acl myacl use-ipv6acl myacl1
switch(config)# show running-config snmp
version 6.2(2)
snmp-server aaa exclusive-behavior enable
snmp-server user admin network-admin auth md5 0x2f2429f3c9b21f1adbae8acc7783e355
priv 0x2f2429f3c9b21f1adbae8acc7783e355 localizedkey
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
snmp-server community newstring group network-operator
snmp-server community newstring use-ipv4acl myacl use-ipv6acl myacl1
switch# show snmp community
Community Group / Access context acl_filter
newstring network-operator ipv4:myacl ipv6:myacl1
switch#
```

Additional References

Related Documents

Related Topic	Document Title
Rollback CLI commands	<i>Cisco Nexus 7000 Series NX-OS System Management Command Reference</i>
VDCs	<i>Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide</i>
IP ACLs and AAA	<i>Cisco Nexus 7000 Series NX-OS Security Configuration Guide</i>
MIBs	<i>Cisco Nexus 7000 Series and 9000 Series NX-OS MIB Quick Reference</i>

RFCs

RFC	Title
RFC 3414	<i>User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)</i>
RFC 3415	<i>View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)</i>

MIBs

MIBs	MIBs Link
MIBs related to SNMP	To locate and download supported MIBs, go to the following URL: ftp://ftp.cisco.com/pub/mibs/supportlists/nexus7000/Nexus7000MIBSupportList.html

Feature History for SNMP

Your software release might not support all the features in this document. For the latest caveats and feature information, see the Bug Search Tool at <https://tools.cisco.com/bugsearch/> and the release notes for your software release.

Table 4: Feature History for SNMP

Feature Name	Releases	Feature Information
SNMPv3 user and communities	6.2(2)	Added the ability to apply both IPv4 and IPv6 ACLs to the same SNMPv3 user or SNMPv3 community.
SNMPv3	6.2(2)	Added support for AAA exclusive behavior in SNMPv3 servers to authenticate users based on location.
SNMP notifications	5.0(2)	Updated the snmp-server enable traps commands.
IPv6 support	4.2(1)	Supports configuring IPv6 SNMP hosts.
Filter SNMP requests by community using an ACL	4.2(1)	Assigns an ACL to an SNMP community to filter SNMP requests.
Use interfaces for SNMP notification receivers	4.2(1)	Added support to designate an interface to act as the source interface for SNMP notifications.
SNMP AAA synchronization	4.0(3)	Added the ability to modify the synchronized user configuration timeout.
SNMP protocol	4.0(3)	Added the ability to disable the SNMP protocol.