



CHAPTER 7

Configuring SNMP

This chapter describes how to configure the SNMP feature on the device.

This chapter includes the following sections:

- [Information About SNMP, page 7-1](#)
- [Licensing Requirements for SNMP, page 7-6](#)
- [Prerequisites for SNMP, page 7-7](#)
- [Configuration Guidelines and Limitations, page 7-7](#)
- [Configuring SNMP, page 7-7](#)
- [Verifying SNMP Configuration, page 7-18](#)
- [SNMP Example Configuration, page 7-18](#)
- [Default Settings, page 7-18](#)
- [Additional References, page 7-19](#)
- [Feature History for SNMP, page 7-20](#)

Information About SNMP

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

This section includes the following topics:

- [SNMP Functional Overview, page 7-2](#)
- [SNMP Notifications, page 7-2](#)
- [SNMPv3, page 7-2](#)
- [SNMP and Embedded Event Manager, page 7-5](#)
- [Multiple Instance Support, page 7-5](#)
- [High Availability, page 7-6](#)
- [Virtualization Support, page 7-6](#)

Send document comments to nexus7k-docfeedback@cisco.com.

SNMP Functional Overview

The SNMP framework consists of three parts:

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

SNMP is defined in RFCs 3411 to 3418.



Note

Cisco NX-OS does not support SNMP sets.

Cisco NX-OS 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 a 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 (see the [“Configuring SNMP Notification Receivers with VRFs”](#) section on page 7-11). 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 NX-OS cannot determine if the trap was received. An SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If Cisco NX-OS never receives a response, it can send the inform request again.

You can configure Cisco NX-OS to send notifications to multiple host receivers. See the [“Configuring SNMP Notification Receivers”](#) section on page 7-10 for more information about host receivers.

SNMPv3

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

- Message integrity—Ensures that a packet has not been tampered with 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.

Send document comments to nexus7k-docfeedback@cisco.com.

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, page 7-3](#)
- [User-Based Security Model, page 7-4](#)
- [CLI and SNMP User Synchronization, page 7-4](#)
- [Group-Based SNMP Access, page 7-5](#)

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 7-1](#) identifies what the combinations of security models and levels mean.

Table 7-1 *SNMP Security Models and Levels*

Model	Level	Authentication	Encryption	What Happens
v1	<code>noAuthNoPriv</code>	Community string	No	Uses a community string match for authentication.
v2c	<code>noAuthNoPriv</code>	Community string	No	Uses a community string match for authentication.
v3	<code>noAuthNoPriv</code>	Username	No	Uses a username match for authentication.
v3	<code>authNoPriv</code>	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	<code>authPriv</code>	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.

Send document comments to nexus7k-docfeedback@cisco.com.

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 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 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 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 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.

Send document comments to nexus7k-docfeedback@cisco.com.

**Note**

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

Cisco NX-OS holds the synchronized user configuration for 60 minutes by default. See the [“Modifying the AAA Synchronization Time”](#) section on page 7-17 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.

SNMP and Embedded Event Manager

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

See [Chapter 10, “Configuring the Embedded Event Manager”](#) for more information about EEM.

Multiple Instance Support

A device can support multiple instances of a logical network entity, such as protocol instances or VRFs. 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 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.

In Cisco NX-OS Release 4.0(2) and later releases, 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.

Send document comments to nexus7k-docfeedback@cisco.com.

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.

To map an SNMP context to a logical network entity, follow these steps:

-
- Step 1** Create the SNMPv3 context.
 - Step 2** Determine the logical network entity instance.
 - Step 3** Map the SNMPv3 context to a logical network entity.
 - Step 4** Optionally, map the SNMPv3 context to an SNMPv2c community.
-

For more information, see the [“Configuring the Context to Network Entity Mapping”](#) section on [page 7-16](#).

High Availability

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

Virtualization Support

Cisco NX-OS supports one instance of the SNMP per virtual device context (VDCs). 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, Release 4.0*

In Cisco NX-OS Release 4.0(2) and later releases, SNMP supports multiple MIB module instances and maps them to logical network entities. For more information, see the [“Multiple Instance Support”](#) section on [page 7-5](#).

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 on [page 7-11](#)).

Licensing Requirements for SNMP

The following table shows the licensing requirements for this feature:

Product	License Requirement
NX-OS	SNMP requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For a complete explanation of the NX-OS licensing scheme, see the <i>Cisco NX-OS Licensing Guide</i> .

Send document comments to nexus7k-docfeedback@cisco.com.

Prerequisites for SNMP

SNMP has the following prerequisites:

- If you configure VDCs, install the Advanced Services license and enter the desired VDC (see the *Cisco NX-OS Virtual Device Context Configuration Guide*).

Configuration Guidelines and Limitations

SNMP has the following configuration guidelines and limitations:

- 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:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

Configuring SNMP

This section includes the following topics:

- [Configuring SNMP Users, page 7-8](#)
- [Enforcing SNMP Message Encryption, page 7-9](#)
- [Assigning SNMPv3 Users to Multiple Roles, page 7-9](#)
- [Creating SNMP Communities, page 7-9](#)
- [Configuring SNMP Notification Receivers, page 7-10](#)
- [Configuring the Notification Target User, page 7-11](#)
- [Configuring SNMP Notification Receivers with VRFs, page 7-11](#)
- [Enabling SNMP Notifications, page 7-12](#)
- [Disabling LinkUp/LinkDown Notifications on an Interface, page 7-14](#)
- [Enabling a One-time Authentication for SNMP over TCP, page 7-14](#)
- [Assigning the SNMP Switch Contact and Location Information, page 7-15](#)
- [Configuring the Context to Network Entity Mapping, page 7-16](#)
- [Disabling SNMP, page 7-17](#)
- [Modifying the AAA Synchronization Time, page 7-17](#)



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.

Send document comments to nexus7k-docfeedback@cisco.com.

Configuring SNMP Users

You can configure a user for SNMP.

BEFORE YOU BEGIN

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

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 switch(config)#	Enters 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 can be any case-sensitive alphanumeric string up to 130 characters. The engineID format is a 12-digit colon-separated decimal number.
Step 3	show snmp user 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 this configuration change.

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

```
switch# config t
switch(config)# snmp-server user Admin auth sha abcd1234 priv abcdefgh
```

Send document comments to nexus7k-docfeedback@cisco.com.

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 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 <i>name</i> 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.

Assigning SNMPv3 Users to Multiple Roles

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



Note

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

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

Command	Purpose
snmp-server user <i>name</i> <i>group</i> Example: switch(config)# snmp-server user Admin superuser	Associates this SNMP user with the configured user role.

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:

Send document comments to nexus7k-docfeedback@cisco.com.

Command	Purpose
<pre>snmp-server community name group {ro rw}</pre> <p>Example: switch(config)# snmp-server community public ro</p>	Creates an SNMP community string.

Configuring SNMP Notification Receivers

You can configure Cisco NX-OS 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
<pre>snmp-server host ip-address traps version 1 community [udp_port number]</pre> <p>Example: switch(config)# snmp-server host 192.0.2.1 traps version 1 public</p>	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
<pre>snmp-server host ip-address {traps informs} version 2c community [udp_port number]</pre> <p>Example: switch(config)# snmp-server host 192.0.2.1 informs version 2c public</p>	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
<pre>snmp-server host ip-address {traps informs} version 3 {auth noauth priv} username [udp_port number]</pre> <p>Example: switch(config)# snmp-server host 192.0.2.1 informs version 3 auth NMS</p>	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 engineID of the Cisco NX-OS device to authenticate and decrypt the SNMPv3 messages.

[Send document comments to nexus7k-docfeedback@cisco.com.](mailto:nexus7k-docfeedback@cisco.com)

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 inform s.

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

Command	Purpose
<pre>snmp-server user name [auth {md5 sha} passphrase [auto] [priv [aes-128] passphrase] [engineID id]</pre> <p>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</p>	<p>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.</p>

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.

Use the following command in global configuration mode to configure a VRF to use for sending notifications to the host receiver:

Command	Purpose
<pre>snmp-server host ip-address use-vrf vrf_name [udp_port number]</pre> <p>Example: switch(config)# snmp-server host 192.0.2.1 use-vrf Blue</p>	<p>Configures SNMP to use the selected VRF to communicate with the host receiver. 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>
<pre>no snmp-server host ip-address use-vrf vrf_name [udp_port number]</pre> <p>Example: switch(config)# no snmp-server host 192.0.2.1 use-vrf Blue</p>	<p>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>Does not remove the host configuration.</p>

Send document comments to nexus7k-docfeedback@cisco.com.

You can configure Cisco NX-OS filter notifications based on the VRF in which the notification occurred. Use the following command in global configuration mode to filter notifications based on a configured VRF:

Command	Purpose
<pre>snmp-server host ip-address filter_vrf vrf_name [udp_port number]</pre> <p>Example: switch(config)# snmp-server host 192.0.2.1 filter_vrf Red</p>	<p>Filters notifications to the notification host receiver based on the configured VRF. 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>
<pre>no snmp-server host ip-address filter_vrf vrf_name</pre> <p>Example: switch(config)# no snmp-server host 192.0.2.1 filter_vrf Red</p>	<p>Removes the VRF filter information for configured host, and removes the entry from the ExtSnmptargetVrfTable of the CISCO-SNMP-TARGET-EXT-MB.</p> <p>This command does not remove the host configuration.</p>

Enabling SNMP Notifications

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

Table 7-2 lists the CLI commands that enable the notifications for Cisco NX-OS MIBs.



Note

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

Table 7-2 Enabling SNMP Notifications

MIB	Related Commands
All notifications	snmp-server enable traps
CISCO-AAA-SERVER-MIB	snmp-server enable traps aaa
CISCO-STP-BRIDGE-MIB	snmp-server enable traps bridge
CISCO-CALLHOME-MIB	snmp-server enable traps callhome
EIGRP4-MIB	snmp-server enable traps eigrp
ENTITY-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

Send document comments to nexus7k-docfeedback@cisco.com.

Table 7-2 Enabling SNMP Notifications (continued)

MIB	Related Commands
SNMPv2-MIB	<code>snmp-server enable traps snmp</code> <code>snmp-server enable traps snmp authentication</code>
CISCO-STPX-MIB	<code>snmp-server enable traps stpx</code>

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 bridge [newroot topologychange] Example: switch(config)# snmp-server enable traps bridge newroot	Enables the STP bridge SNMP notifications.
snmp-server enable traps callhome Example: switch(config)# snmp-server enable traps callhome	Enables the CISCO-CALLHOME-MIB SNMP notifications.
snmp-server enable traps eigrp Example: switch(config)# snmp-server enable traps eigrp	Enables the EIGRPv4-MIB 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.

Send document comments to nexus7k-docfeedback@cisco.com.

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.
snmp-server enable traps stpx [inconsistency loop-inconsistency root-inconsistency] Example: switch(config)# snmp-server enable traps stpx root-inconsistency	Enables the STPX SNMP 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.

Send document comments to nexus7k-docfeedback@cisco.com.

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

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

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 switch(config)#	Enters configuration mode.
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	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 this configuration change.

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

```
switch# config t
switch(config)# snmp contact Admin
switch(config)# snmp location Lab-7
```

[Send document comments to nexus7k-docfeedback@cisco.com.](mailto:nexus7k-docfeedback@cisco.com)

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

Ensure that you are in the correct VDC (or use the **switchto vdc** command).

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, Release 4.0* or the *Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide, Release 4.0*.

SUMMARY STEPS

1. **config t**
2. **snmp-server context** *context-name* [**instance** *instance-name*] [**vrf** *vrf-name*] [**topology** *topology-name*]
3. **snmp-server mib community-map** *community-name* **context** *context-name*
4. **show snmp context**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	config t Example: switch# config t switch(config)#	Enters configuration mode.
Step 2	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. The names can be any alphanumeric string up to 32 characters.
Step 3	snmp-server mib community-map <i>community-name</i> context <i>context-name</i> Example: switch(config)# snmp-server mib community-map public context public1	(Optional) Maps an SNMPv2c community to an SNMP context. The names can be any alphanumeric string up to 32 characters.
Step 4	show snmp context Example: switch(config)# show snmp	(Optional) Displays information about one or more SNMP contexts.
Step 5	copy running-config startup-config Example: switch(config)# copy running-config startup-config	(Optional) Saves this configuration change.

Send document comments to nexus7k-docfeedback@cisco.com.

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

```
switch# config t
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# config t
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
```

Use the following command in global configuration mode to delete the mapping between an SNMP context and a logical network entity:

Command	Purpose
<pre>no snmp-server context context-name [instance instance-name] [vrf vrf-name] [topology topology-name]</pre> <p>Example: switch(config)# no snmp-server context public1</p>	<p>Deletes the mapping between an SNMP context and a protocol instance, VRF, or topology. The names can be any alphanumeric string up to 32 characters.</p> <p>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.</p>

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
<pre>no snmp-server protocol enable</pre> <p>Example: switch(config)# no snmp-server protocol enable</p>	<p>Disables the SNMP protocol. This command is enabled by default.</p>

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:

Send document comments to nexus7k-docfeedback@cisco.com.

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 SNMP Configuration

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

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 Cisco NX-OS to send 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
  
```

Default Settings

Table 7-3 lists the default settings for SNMP parameters.

Send document comments to nexus7k-docfeedback@cisco.com.

Table 7-3 **Default SNMP Parameters**

Parameters	Default
license notifications	enabled

Additional References

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

- [Related Documents, page 7-20](#)
- [Standards, page 7-20](#)
- [MIBs, page 7-20](#)

Send document comments to nexus7k-docfeedback@cisco.com.

Related Documents

Related Topic	Document Title
SNMP CLI commands	<i>Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 4.0</i> at the following URL: http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/system_management/configuration/guide/sm_nx-os_config.html
VDCs and VRFs	<i>Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 4.0</i> at the following URL: http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/virtual_device_context/configuration/guide/vdc_nx-os_book.html
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

MIBs	MIBs Link
<ul style="list-style-type: none"> • SNMP-COMMUNITY-MIB • SNMP-FRAMEWORK-MIB • SNMP-NOTIFICATION-MIB • SNMP-TARGET-MIB • SNMPv2-MIB 	To locate and download MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

Feature History for SNMP

Table 7-4 lists the release history for this feature.

Table 7-4 Feature History for SNMP

Feature Name	Releases	Feature Information
SNMP AAA synchronization	4.0(3)	Added ability to modify the synchronized user configuration timeout.
SNMP protocol	4.0(3)	Added ability to disable the SNMP protocol.