Configuring SNMP

This chapter contains the following sections:

Information About SNMP

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network. SNMP supports IPv4 and IPv6 addresses.

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

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

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

SNMPv3

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

- Message integrity—Ensures that a packet has not been tampered with while it was in-transit.
- Authentication—Determines 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.

Note noAuthnoPriv is not supported in SNMPv3.

The following table lists identifies the combinations of security models and level information.

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	authNoPriv	HMAC-MD5 or HMAC-SHA	No	Provides authentication based on the Hash-Based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm or the HMAC Secure Hash Algorithm (SHA).
v3	authPriv	HMAC-MD5 or HMAC-SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.

User-Based Security Model

SNMPv3 User-Based Security Model (USM) refers to SNMP message-level security and offers the following services:

- Message integrity—Ensures that messages have not been altered or destroyed in an unauthorized manner and that data sequences have not been altered to an extent greater than can occur nonmaliciously.
- Message origin authentication—Ensures that the claimed identity of the user on whose behalf received data was originated is confirmed.
- Message confidentiality—Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

SNMPv3 authorizes management operations only by configured users and encrypts SNMP messages.

Cisco NX-OS uses two authentication protocols for SNMPv3:

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

The 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 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 cleartext, 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. After user authentication is verified, the SNMP PDUs are processed. 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 a 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 delete a user using either SNMP or the CLI, the user is deleted for both SNMP and the CLI.
- User-role mapping changes are synchronized in SNMP and the CLI.
- Role changes (deletions or modifications) from the CLI are synchronized to SNMP.

Note When you configure passphrase/password in localized key/encrypted format, Cisco 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. For information about how to modify this default value, see Modifying the AAA Synchronization Time, on page 16.

Group-Based SNMP Access

Note Because group is a standard SNMP term used industry-wide, roles are referred 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.

High Availability

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

Guidelines and Limitations for SNMP

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

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

- SNMP role based access control (RBAC) is not supported.
- The SNMP set command is supported by the following Cisco MIBs:
  - CISCO-IMAGE-UPGRADE-MIB
  - CISCO-CONFIG-COPY-MIB
- The recommended SNMP polling interval time is 5 minutes.

Default Settings for SNMP

Parameters	Default
license notifications	enabled

Configuring SNMP

This section includes the following topics:

- Configuring SNMP
- Users Enforcing SNMP Message Encryption
- Creating SNMP Communities
- Configuring SNMP Notification Receivers
- Configuring the Notification Target User
- Enabling SNMP Notifications
- Disabling LinkUp/LinkDown Notifications on an Interface
- Enabling a One-time Authentication for SNMP over TCP
- Assigning the SNMP Switch Contact and Location Information
- Disabling SNMP

- Modifying the AAA Synchronization Time

Configuring SNMP Users

Before you begin

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*] [**localizedkey**]]	Configures an SNMP user with authentication and privacy parameters. 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 *name* argument is the name of a user who can access the SNMP engine. The **auth** keyword enables one-time authentication for SNMP over a TCP session. It is optional. The **md5** keyword specifies the HMAC MD5 algorithm for authentication. It is optional. The **sha** keyword specifies the HMAC SHA algorithm for authentication. It is optional. The **priv** keyword specifies encryption parameters for the user. It is optional. The **aes-128** keyword specifies the 128-byte AES algorithm for privacy. It is optional. The **engineID** keyword specifies the engineID for configuring the notification target user (for V3 informs). It is optional. The *id* is a 12-digit colon-separated decimal number.
Step 3	(Optional) switch(config-callhome)# **show snmp user**	Displays information about one or more SNMP users.
Step 4	(Optional) switch(config-callhome)# **copy running-config startup-config**	Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Example

This example shows how to configure a SNMP user:

```
switch(config)# configure terminal
switch(config)# snmp-server user Admin auth sha Axlm1234# priv Axlm1234#
switch(config)# show snmp user

_____________________________________________________________________
SNMP USERS
_____________________________________________________________________
User Auth Priv(enforce) Groups
____ ____ _____________ ______
Admin sha des(no) network-operator
admin md5 des(no) network-admin

_____________________________________________________________________
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
_____________________________________________________________________
User Auth Priv
____ ____ ____
switch(config)#
```

Enforcing SNMP Message Encryption for All Users

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **snmp-server globalEnforcePriv**	Enforces SNMP message encryption for all users.

Example

This example shows how to enforce the SNMP message encryption:

```
switch# configure terminal
switch(config)# snmp-server galobalEnforcePriv
switch(config)# show snmp user

_____________________________________________________________________
SNMP USERS [global privacy flag enabled]
_____________________________________________________________________

User                          Auth  Priv(enforce) Groups
____                          ____  _____________ ______
Admin                         sha   des(no)       network-operator

admin                         md5   des(no)       network-admin

_____________________________________________________________________
 NOTIFICATION TARGET USERS (configured  for sending V3 Inform)
_____________________________________________________________________

User                          Auth  Priv
____                          ____  ____
switch(config)#
```

Creating SNMP Communities

You can create SNMP communities for SNMPv1 or SNMPv2c.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **snmp-server community** *name* {**ro** | **rw**}	Creates an SNMP community string.

Example

This example shows how to create an SNMP community:

```
switch# configure terminal
switch(config)# snmp-server community public ro
switch(config)# show snmp community
Community Group / Access context acl_filter
------------------------------ -------------- ------- ----------
public network-operator
switch(config)#
```

Filtering SNMP Requests

You can assign an access list (ACL) to a community to filter incoming SNMP requests. If the assigned ACL allows the incoming request packet, SNMP processes the request. If the ACL denies the request, SNMP drops the request and sends a system message. The ACL applies to IPv4 and IPv6 over UDP and TCP. After creating the ACL, assign the ACL to the SNMP community. For more information on creating ACLs, see the *Cisco Nexus 1000V for VMware Security Configuration Guide*.

Before you begin

Create an ACL to assign to the SNMP community. Assign the ACL to the SNMP community. 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	switch# **configure terminal**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	switch(config-callhome)# **snmp-server community** *community-name* **use-acl** *acl-name*	Assigns an ACL to an SNMP community to filter SNMP requests.
Step 3	switch(config-callhome)# {**ip** | **ipv6**} **access-list acl_for_community**	Configures an IP ACL.
Step 4	switch(config-callhome)# **statistics per-entry**	Configures statistics.
Step 5	switch(config-callhome)# **permit udp any any**	Permits UDP protocol.
Step 6	(Optional) switch(config-callhome)# **show** {**ip** | **ipv6**} **access-lists**	Displays **show** command output.
Step 7	switch(config-callhome)# **snmp-server community public use-acl acl_for_community**	Configures SNMP community.
Step 8	(Optional) switch(config-callhome)# **showsnmp community**	Displays **show** command output.

Example

This example shows how to filter SNMP requests:

```
switch# configure terminal
switch(config)# show ip access-lists
IPV4 ACL acl_for_community
statistics per-entry
10 permit udp any any
switch(config)# show snmp community
Community Group / Access context acl_filter
------------------------------ -------------- ------- ----------
public network-operator acl_for_community
```

Configuring SNMP Notification Receivers

Configuring a Host Receiver for SNMPv1 Traps

Before you begin

You must be in global configuration mode.

Procedure

	Command or Action	Purpose
Step 1	switch(config)# **snmp-server host** *ip-address* **traps version 1** *community* [**udp_port** *number*]	Configures a host receiver for SNMPv1 traps. You can specify an IPv4 or IPv6 address. The community can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

Example

```
switch(config)# snmp-server host 192.0.2.1 traps version 1 public
switch(config)# show snmp host
-------------------------------------------------------------------
Host                            Port Version  Level  Type   SecName

-------------------------------------------------------------------
192.0.2.1                       162  v1       noauth trap   public

-------------------------------------------------------------------
switch(config)#
```

Configuring a Host Receiver for SNMPv2c Traps or Informs

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **snmp-server host** *ip-address* {**traps** | **informs**} **version 2c** *community* [**udp_port** *number*]	Configures a host receiver for SNMPv2c traps or informs. You can specify an IPv4 or IPv6 address. The community can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

Example

```
switch# configure terminal
switch(config)# snmp-server host 192.0.2.1 informs version 2c public
switch(config)# show snmp host
-------------------------------------------------------------------
Host                            Port Version  Level  Type   SecName

-------------------------------------------------------------------
192.0.2.1                       162  v2c      noauth inform public

-------------------------------------------------------------------
switch(config)#
```

Configuring a Host Receiver for SNMPv3 Traps or Informs

Note The SNMP manager must know the user credentials (authKey/PrivKey) based on the SNMP engine ID of the Cisco Nexus 1000V device to authenticate and decrypt the SNMPv3 messages

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **snmp-server host** *ip-address* {**traps** | **informs**} **version 3** {**auth** | **noauth** | **priv**} *username* [**udp_port** *number*]	Configures a host receiver for SNMPv2c traps or informs. You can specify an IPv4 or IPv6 address. The username can be any alphanumeric string up to 255 characters. The UDP port number range is from 0 to 65535.

Example

This example shows how to configure a host receiver:

```
switch# configure terminal
switch# configure terminal
switch(config)# snmp-server host 192.0.2.1 informs version 3 auth Admin
switch(config)# show snmp host
-------------------------------------------------------------------
Host Port Version Level Type SecName
-------------------------------------------------------------------
192.0.2.1 162 v3 auth inform Admin
-------------------------------------------------------------------
switch(config)#
```

Configuring the Notification Target User

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

The Cisco 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	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **snmp-server user** *name* [**auth** {**md5** | **sha**} *passphrase* [**auto**] [**priv** [**aes-128**] *passphrase*] [**engineID** *id*]	Configures the notification target user with the specified engine ID for notification host receiver. The *id* is a 12-digit colon-separated decimal number.

Example

This example shows how to configure a notification target user:

```
switch# configure terminal
switch(config)# snmp-server user Admin auth sha Axlm1234# priv Axlm1234#
engineID 00:00:00:63:00:01:00:10:20:15:10:03
switch(config)# show snmp user
_____________________________________________________________________
SNMP USERS [global privacy flag enabled]
_____________________________________________________________________
User Auth Priv(enforce) Groups
____ ____ _____________ ______
admin md5 des(no) network-admin
_____________________________________________________________________
NOTIFICATION TARGET USERS (configured for sending V3 Inform)
_____________________________________________________________________
User Auth Priv
____ ____ ____
Admin sha des
(EngineID 0:0:0:63:0:1:0:10:20:15:10:3)
switch(config)#
```

Enabling SNMP Notifications

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

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

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

MIB	Related Commands
All notifications	**snmp-server enable traps**
CISCO-AAA-SERVER-MIB	**snmp-server enable traps aaa**
ENITY-MIB	**snmp-server enable traps entity**
CISCO-ENTITY-FRU-CONTROL-MIB	**snmp-server enable traps entity fru**
CISCO-LICENSE-MGR-MIB	**snmp-server enable traps license**
IF-MIB	**snmp-server enable traps link**
SNMPv2-MIB	**snmp-server enable traps snmp** **snmp-server enable traps snmp authentication**

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

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **snmp-server enable traps**	Enables all SNMP notifications.
Step 3	switch(config)# **snmp-server enable traps aaa** [**server-state-change**]	Enables the AAA SNMP notifications.
Step 4	switch(config)# **snmp-server enable traps entity** [**fru**]	Enables the ENTITY-MIB SNMP notifications.
Step 5	switch(config)# **snmp-server enable traps license**	Enables the license SNMP notification.
Step 6	switch(config)# **snmp-server enable traps link**	Enables the link SNMP notifications.
Step 7	switch(config)# **snmp-server enable traps snmp** [**authentication**]	Enables the SNMP agent notifications.

Example

This example displays how to enable SNMP notifications:

```
switch# configure terminal
switch(config)# snmp-server enable traps
switch(config)# snmp-server enable traps aaa
switch(config)# snmp-server enable traps entity
switch(config)# snmp-server enable traps license
switch(config)# snmp-server enable traps link
switch(config)# snmp-server enable traps snmp
```

Disabling LinkUp/LinkDown Notifications on an Interface

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

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config-if)# **no snmp trap link-status**	Disables SNMP link-state traps for the interface. This command is enabled by default.

Example

```
switch# show running-config interface vethernet 1
interface Vethernet1
inherit port-profile
dynpp_d50369db-2fed-405d-ad84-a6bf89718d2c_f006e797-da04-4f29-9a0f-901294bc8b8f
```

```
description TEST, Network Adapter
dvport uuid "70D66D72-CDD9-4B68-9596-27E8F8E06F6D--0"
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# interface vethernet 1
switch(config-if)# no snmp trap link-status
switch(config-if)# show running-config interface vethernet 1
interface Vethernet1
inherit port-profile
dynpp_d50369db-2fed-405d-ad84-a6bf89718d2c_f006e797-da04-4f29-9a0f-901294bc8b8f
description TEST, Network Adapter
dvport uuid "70D66D72-CDD9-4B68-9596-27E8F8E06F6D--0"
no snmp trap link-status
```

Enabling a One-time Authentication for SNMP over TCP

Before you begin

You must be in global configuration mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **snmp-server tcp-session** [**auth**]	Enables a one-time authentication for SNMP over a TCP session. The default is disabled.

Example

This example shows how to enable a one -time authentication:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server tcp-session
switch(config)# show snmp | grep "Tcp"
SNMP Tcp Authentication Flag : Enabled.
switch(config)#
```

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

Log in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **snmp-server contact** *name*	Configures sysContact, which is the SNMP contact name.
Step 3	switch(config)# **snmp-server location** *name*	Configures sysLocation, which is the SNMP location.
Step 4	(Optional) switch(config)# **show snmp**	Displays information about one or more destination profiles.
Step 5	(Optional) switch(config)# **copy running-config startup-config**	Saves the change persistently through reboots and restarts by copying the running configuration to the startup configuration.

Example

This example show how to assign information on the SNMP switch contact and location:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# snmp-server contact Admin
switch(config)# snmp-server location Lab
switch(config)# show snmp | grep sys
sys contact: Admin
sys location: Lab
switch(config)# copy running-config startup-config
```

Disabling SNMP

Procedure

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

Example

This example shows how to disable the SNMP protocol:

```
switch# configure terminal
switch(config)# no snmp-server protocol enable
switch(config)# show snmp | grep protocol
SNMP protocol : Disabled
switch(config)#
```

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	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **snmp-server aaa-user cache-timeout** *seconds*	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.

Example

This example shows how to modify the AAA synchronization time:

```
switch# configure terminal
switch(config)# snmp-server aaa-user cache-timeout 1200
```

Verifying the SNMP Configuration

Use one of the following commands to verify the configuration:

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 session	Displays SNMP sessions.
show snmp trap	Displays the SNMP notifications that are enabled or disabled.
show snmp user	Displays SNMPv3 users.
show snmp host	Displays information about configured SNMP hosts.

Configuration Example for SNMP

This example shows how to configure Cisco NX-OS to send linkUp/Down notifications to one notification host receiver.

```
switch(config)# snmp-server user Admin auth sha Axlm1234# priv Axlm1234#
switch(config)# snmp-server host 192.0.2.1 traps version 3 priv Admin
switch(config)# snmp-server enable traps link
switch(config)# show snmp user

_______________________________________________________________________
SNMP USERS [global privacy flag enabled]

_______________________________________________________________________
User Auth Priv(enforce) Groups

____ ____ _____________ ______
Admin sha des(no) network-operator
admin md5 des(no) network-admin

_______________________________________________________________________
NOTIFICATION TARGET USERS (configured for sending V3 Inform)

_______________________________________________________________________
User Auth Priv

____ ____ ____
switch(config)# show snmp host
-------------------------------------------------------------------
Host Port Version Level Type SecName
-------------------------------------------------------------------
192.0.2.1 162 v3 priv trap Admin
-------------------------------------------------------------------
switch(config)# show snmp trap | grep link
link : linkDown Yes
link : linkUp Yes
link : extended-linkDown Yes
link : extended-linkUp Yes
link : cieLinkDown Yes
link : cieLinkUp Yes
link : cisco-xcvr-mon-status-chg Yes
switch(config)#
```

MIBs

The supported SNMP MIBs are listed in this section.

To locate and download the MIBs, go to the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

- IF-MIB
- ENTITY-MIB
- CISCO-ENTITY-EXT-MIB-V1SMI
- CISCO-ENTITY-FRU-CONTROL-MIB
- BRIDGE-MIB
- CISCO-FLASH-MIB
- CISCO-SYSTEM-MIB

- CISCO-SYSTEM-EXT-MIB
- CISCO-FEATURE-CONTROL-MIB
- CISCO-CDP-MIB
- CISCO-VIRTUAL-NIC-MIB
- CISCO-PROCESS-MIB
- CISCO-SYSLOG-EXT-MIB
- CISCO-VLAN-MEMBERSHIP-MIB
- TCP-MIB
- UDP-MIB
- CISCO-PRIVATE-VLAN-MIB
- CISCO-SECURE-SHELL-MIB
- CISCO-IMAGE-UPGRADE-MIB
- CISCO-LICENSE-MGR-MIB
- RMON2-MIB
- CISCO-AAA-SERVER-MIB
- CISCO-AAA-SERVER-EXT-MIB
- CISCO-COMMON-MGMT-MIB
- CISCO-COMMON-ROLES-MIB
- CISCO-CONFIG-MAN-MIB
- CISCO-FTP-CLIENT-MIB
- CISCO-IMAGE-MIB
- CISCO-LAG-MIB
- CISCO-NOTIFICATION-CONTROL-MIB
- CISCO-NTP-MIB
- CISCO-RF-MIB
- CISCO-RMON-CONFIG-MIB
- CISCO-SMI
- CISCO-SNMP-TARGET-EXT-MIB
- NOTIFICATION-LOG-MIB
- IP-MIB
- SNMP-COMMUNITY-MIB
- SNMP-FRAMEWORK-MIB

- SNMP-MPD-MIB
- SNMP-NOTIFICATION-MIB
- SNMP-TARGET-MIB
- SNMP-USM-MIB
- SNMPv2-MIB

Feature History for SNMP

Feature Name	Releases	Feature Information
IPv6	5.2(1)SV3(1.1)	SNMP supports IPv6 addresses.
SNMP	4.0(4)SV1(1)	This feature was introduced.