



## CHAPTER 7

# Configuring SNMP

The CLI and SNMP use common roles in all switches in the Cisco MDS 9000 Family. You can use SNMP to modify a role that was created using the CLI and vice versa.

Users, passwords, and roles for all CLI and SNMP users are the same. A user configured through the CLI can access the switch using SNMP (for example, the Fabric Manager or the Device Manager) and vice versa.

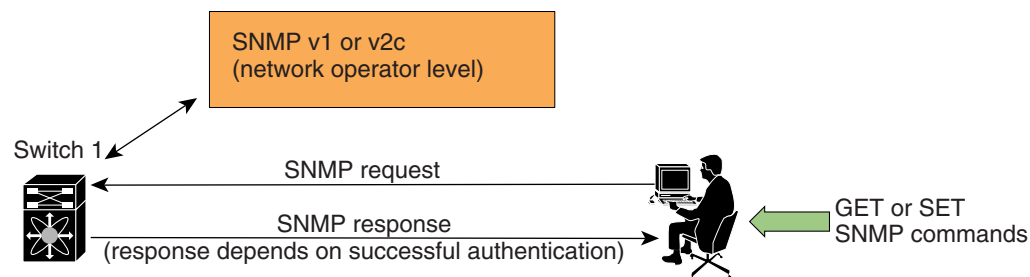
This chapter includes the following sections:

- [About SNMP Security, page 7-1](#)
- [SNMPv3 CLI User Management and AAA Integration, page 7-3](#)
- [Creating and Modifying Users, page 7-4](#)
- [SNMP Trap and Inform Notifications, page 7-8](#)
- [Default Settings, page 7-19](#)

## About SNMP Security

SNMP is an application layer protocol that facilitates the exchange of management information between network devices. In all Cisco MDS 9000 Family switches, three SNMP versions are available: SNMPv1, SNMPv2c, and SNMPv3 (see [Figure 7-1](#)).

**Figure 7-1** *SNMP Security*



85473

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

This section includes the following topics:

- [SNMP Version 1 and Version 2c, page 7-2](#)
- [SNMP Version 3, page 7-2](#)
- [Assigning SNMP Switch Contact and Location Information, page 7-2](#)

## SNMP Version 1 and Version 2c

SNMP Version 1 (SNMPv1) and SNMP Version 2c (SNMPv2c) use a community string match for user authentication. Community strings provided a weak form of access control in earlier versions of SNMP. SNMPv3 provides much improved access control using strong authentication and should be preferred over SNMPv1 and SNMPv2c wherever it is supported.

## SNMP Version 3

SNMP Version 3 (SNMPv3) is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. The security features provided in SNMPv3 are:

- 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.

## Assigning SNMP Switch Contact and Location Information

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

To configure contact and location information, follow these steps:

|        | Command                                                | Purpose                                  |
|--------|--------------------------------------------------------|------------------------------------------|
| Step 1 | switch# <b>config t</b>                                | Enters configuration mode.               |
| Step 2 | switch(config)# <b>snmp-server contact NewUser</b>     | Assigns the contact name for the switch. |
|        | switch(config)# <b>no snmp-server contact NewUser</b>  | Deletes the contact name for the switch. |
| Step 3 | switch(config)# <b>snmp-server location SanJose</b>    | Assigns the switch location.             |
|        | switch(config)# <b>no snmp-server location SanJose</b> | Deletes the switch location.             |

*Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)*

## SNMPv3 CLI User Management and AAA Integration

The Cisco NX-OS software implements RFC 3414 and RFC 3415, including user-based security model (USM) and role-based access control. While SNMP and the CLI have common role management and share the same credentials and access privileges, the local user database was not synchronized in earlier releases.

SNMPv3 user management can be centralized at the AAA server level. This centralized user management allows the SNMP agent running on the Cisco MDS switch to leverage the user authentication service of the AAA server. Once user authentication is verified, the SNMP PDUs are processed further. The AAA server also is used to store user group names. SNMP uses the group names to apply the access/role policy that is locally available in the switch.

This section includes the following topics:

- [CLI and SNMP User Synchronization, page 7-3](#)
- [Restricting Switch Access, page 7-3](#)
- [Group-Based SNMP Access, page 7-4](#)

### CLI and SNMP User Synchronization

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

To create an SNMP or CLI user, use either the **username** or **snmp-server user** commands.

- The auth passphrase specified in the **snmp-server user** command is synchronized as the password for the CLI user.
- The password specified in the **username** command is synchronized as the auth and priv passphrases for the SNMP user.

Users are synchronized as follows:

- Deleting a user using either command results in the user being deleted for both SNMP and the CLI.
- User-role mapping changes are synchronized in SNMP and the CLI.



**Note** When the passphrase/password is specified in localized key/encrypted format, the password is not synchronized.

- Existing SNMP users continue to retain the auth and priv passphrases without any changes.
- If the management station creates an SNMP user in the `usmUserTable`, the corresponding CLI user is created without any password (login is disabled) and will have the `network-operator` role.

### Restricting Switch Access

You can restrict access to a Cisco MDS 9000 Family switch using IP Access Control Lists (IP-ACLs).

**[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

## Group-Based SNMP Access



### Note

Because *group* is a standard SNMP term used industry-wide, we refer to role(s) as group(s) in this SNMP section.

SNMP access rights are organized by groups. Each group in SNMP is similar to a role through the CLI. Each group is defined with three accesses: read access, write access, and notification access. Each access can be enabled or disabled within each group.

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

## Creating and Modifying Users

You can create users or modify existing users using SNMP, Fabric Manager, or the CLI.

- **SNMP**—Create a user as a clone of an existing user in the `usmUserTable` on the switch. Once you have created the user, change the cloned secret key before activating the user. Refer to RFC 2574.
- **Fabric Manager.**
- **CLI**—Create a user or modify an existing user using the **`snmp-server user`** command.

A `network-operator` and `network-admin` roles are available in a Cisco MDS 9000 Family switch. There is also a default-role if you want to use the GUI (Fabric Manager and Device Manager). You can also use any role that is configured in the Common Roles database.



### Tip

All updates to the CLI security database and the SNMP user database are synchronized. You can use the SNMP password to log into either Fabric Manager or Device Manager. However, after you use the CLI password to log into Fabric Manager or Device Manager, you must use the CLI password for all future logins. If a user exists in both the SNMP database and the CLI database before upgrading to Cisco MDS SAN-OS Release 2.0(1b), then the set of roles assigned to the user becomes the union of both sets of roles after the upgrade.

This section includes the following topics:

- [About AES Encryption-Based Privacy, page 7-4](#)
- [Configuring SNMP Users from the CLI, page 7-5](#)
- [Enforcing SNMPv3 Message Encryption, page 7-6](#)
- [Assigning SNMPv3 Users to Multiple Roles, page 7-7](#)
- [Adding or Deleting Communities, page 7-7](#)

## About AES Encryption-Based Privacy

The Advanced Encryption Standard (AES) is the symmetric cipher algorithm. The Cisco NX-OS software uses AES as one of the privacy protocols for SNMP message encryption and conforms with RFC 3826.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

The **priv** option offers a choice of DES or 128-bit AES encryption for SNMP security encryption. The **priv** option along with the **aes-128** token indicates that this privacy password is for generating a 128-bit AES key. The AES priv password can have a minimum of eight characters. If the passphrases are specified in clear text, you can specify a maximum of 64 characters. If you use the localized key, you can specify a maximum of 130 characters.



**Note**

For an SNMPv3 operation using the external AAA server, user configurations in the external AAA server require AES to be the privacy protocol to use SNMP PDU encryption.

## Configuring SNMP Users from the CLI

The passphrase specified in the **snmp-server user** command and the **username** command are synchronized.

To create or modify SNMP users from the CLI, follow these steps:

|        | Command                                                                                                      | Purpose                                                                                                                                                    |
|--------|--------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | switch# <b>config t</b><br>switch(config)#                                                                   | Enters configuration mode.                                                                                                                                 |
| Step 2 | switch(config)# <b>snmp-server user joe network-admin auth sha abcd1234</b>                                  | Creates or modifies the settings for a user (joe) in the network-admin role using the HMAC-SHA-96 authentication password (abcd1234).                      |
|        | switch(config)# <b>snmp-server user sam network-admin auth md5 abcdefgh</b>                                  | Creates or modifies the settings for a user (sam) in the network-admin role using the HMAC-MD5-96 authentication password (abcdefgh).                      |
|        | switch(config)# <b>snmp-server user Bill network-admin auth sha abcd1234 priv abcdefgh</b>                   | Creates or modifies the settings for a user (Bill) in the network-admin role using the HMAC-SHA-96 authentication level and privacy encryption parameters. |
|        | switch(config)# <b>no snmp-server user usernameA</b>                                                         | Deletes the user (usernameA) and all associated parameters.                                                                                                |
|        | switch(config)# <b>no snmp-server usam role vsan-admin</b>                                                   | Deletes the specified user (usam) from the vsan-admin role.                                                                                                |
|        | switch(config)# <b>snmp-server user user1 network-admin auth md5 0xab0211gh priv 0x45abf342 localizedkey</b> | Specifies the password to be in localized key format (RFC 2574). The localized key is provided in hexadecimal format (for example, 0xacbdef).              |
|        | switch(config)# <b>snmp-server user user2 auth md5 asdgfsadf priv aes-128 asgfsghkhkj</b>                    | Configures the user2 with the MD5 authentication protocol and AES-128 privacy protocol.                                                                    |
| Step 3 | switch(config)# <b>snmp-server user joe sangroup</b>                                                         | Adds the specified user (joe) to the sangroup role.                                                                                                        |
|        | switch(config)# <b>snmp-server user joe techdocs</b>                                                         | Adds the specified user (joe) to the techdocs role.                                                                                                        |

## Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

To create or modify passwords for SNMP users from the CLI, follow these steps:

|        | Command                                                                                                      | Purpose                                                                                                   |
|--------|--------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| Step 1 | switch# <b>config t</b><br>switch(config)#                                                                   | Enters configuration mode.                                                                                |
| Step 2 | switch(config)# <b>snmp-server user user1 role1 auth md5 0xab0211gh priv 0x45abf342 localizedkey</b>         | Specifies the password to be in localized key format using the DES option for security encryption.        |
|        | switch(config)# <b>snmp-server user user1 role2 auth sha 0xab0211gh priv aes-128 0x45abf342 localizedkey</b> | Specifies the password to be in localized key format using the 128-bit AES option for security encryption |



### Caution

Avoid using the **localizedkey** option when configuring an SNMP user from the CLI. The localized keys are not portable across devices as they contain device engine ID information. If a configuration file is copied to the device, the passwords may not be set correctly if the configuration file was generated at a different device. Explicitly configure the desired passwords after copying the configuration into the device. Passwords specified with the **localizedkey** option are limited to 130 characters.



### Note

The **snmp-server user** command takes the engineID as an additional parameter. The engineID creates the notification target user (see the “[Configuring the Notification Target User](#)” section on page 7-13). If the engineID is not specified, the local user is created.

## Enforcing SNMPv3 Message Encryption

By default the SNMP agent allows the securityLevel parameters of authNoPriv and authPriv for the SNMPv3 messages that use user-configured SNMPv3 message encryption with auth and priv keys.

To enforce the message encryption for a user, follow these steps:

|        | Command                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | switch# <b>config t</b><br>switch(config)#                      | Enters configuration mode.                                                                                                                                                                                                                                                                                                                                                                   |
| Step 2 | switch(config)# <b>snmp-server user testUser enforcePriv</b>    | Enforces the message encryption for SNMPv3 messages using this user.<br><br><b>Note</b> You can only use this command for previously existing users configured with both auth and priv keys. When the user is configured to enforce privacy, for any SNMPv3 PDU request using securityLevel parameter of either noAuthNoPriv or authNoPriv, the SNMP agent responds with authorizationError. |
|        | switch(config)# <b>no snmp-server user testUser enforcePriv</b> | Disables SNMPv3 message encryption enforcement.                                                                                                                                                                                                                                                                                                                                              |

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

Alternatively, you can enforce the SNMPv3 message encryption globally on all the users using the following commands:

|        | Command                                                 | Purpose                                                                 |
|--------|---------------------------------------------------------|-------------------------------------------------------------------------|
| Step 1 | switch# <b>config t</b><br>switch(config)#              | Enters configuration mode.                                              |
| Step 2 | switch(config)# <b>snmp-server globalEnforcePriv</b>    | Enforces the SNMPv3 message encryption for all the users on the switch. |
|        | switch(config)# <b>no snmp-server globalEnforcePriv</b> | Disables global SNMPv3 message encryption enforcement.                  |

## Assigning SNMPv3 Users to Multiple Roles

The SNMP server user configuration is enhanced to accommodate multiple roles (groups) for SNMPv3 users. After the initial SNMPv3 user creation, you can map additional roles for the user.



### Note

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

To configure multiple roles for SNMPv3 users from the CLI, follow these steps:

|        | Command                                                | Purpose                                                                           |
|--------|--------------------------------------------------------|-----------------------------------------------------------------------------------|
| Step 1 | switch# <b>config t</b><br>switch(config)#             | Enters configuration mode.                                                        |
| Step 2 | switch(config)# <b>snmp-server user NewUser role1</b>  | Creates or modifies the settings for an SNMPv3 user (NewUser) for the role1 role. |
|        | switch(config)# <b>snmp-server user NewUser role2</b>  | Creates or modifies the settings for an SNMPv3 user (NewUser) for the role2 role. |
|        | switch(config)# <b>no snmp-server user User5 role2</b> | Removes role2 for the specified user (User5).                                     |

## Adding or Deleting Communities

You can configure read-only or read-write access for SNMPv1 and SNMPv2 users. Refer to RFC 2576.

To create an SNMPv1 or SNMPv2c community, follow these steps:

|        | Command                                                        | Purpose                                                    |
|--------|----------------------------------------------------------------|------------------------------------------------------------|
| Step 1 | switch# <b>config t</b>                                        | Enters configuration mode.                                 |
| Step 2 | switch(config)# <b>snmp-server community snmp_Community ro</b> | Adds read-only access for the specified SNMP community.    |
|        | switch(config)# <b>snmp-server community snmp_Community rw</b> | Adds read-write access for the specified SNMP community.   |
|        | switch(config)# <b>no snmp-server community snmp_Community</b> | Deletes access for the specified SNMP community (default). |

[Send documentation comments to mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)

## SNMP Trap and Inform Notifications

You can configure the Cisco MDS switch to send notifications to SNMP managers when particular.



### Note

You must enable the RMON traps in the SNMP configuration. For more information refer to [Configuring RMON, page 8-2](#)

Use the SNMP-TARGET-MIB to obtain more information on the destinations to which notifications are to be sent either as traps or as informs. Refer to the *Cisco MDS 9000 Family MIB Quick Reference*.

This section includes the following topics:

- [Configuring SNMPv2c Notifications, page 7-8](#)
- [Configuring SNMPv3 Notifications, page 7-9](#)
- [Enabling SNMP Notifications, page 7-10](#)
- [Configuring the Notification Target User, page 7-13](#)
- [Configuring LinkUp/LinkDown Notifications for Switches, page 7-13](#)
- [Configuring Up/Down SNMP Link-State Traps for Interfaces, page 7-15](#)
- [Displaying SNMP Security Information, page 7-17](#)



### Tip

The SNMPv1 option is not available with the **snmp-server host ip-address informs** command.

## Configuring SNMPv2c Notifications

To configure SNMPv2c notifications using IPv4, follow these steps:

|        | Command                                                                                            | Purpose                                                                                                                         |
|--------|----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | switch# <b>config t</b><br>switch(config)#                                                         | Enters configuration mode.                                                                                                      |
| Step 2 | switch(config)# <b>snmp-server host 171.71.187.101 traps version 2c private udp-port 1163</b>      | Configures the specified host to receive SNMPv2c traps using SNMPv2c community string (private).                                |
|        | switch(config)# <b>no snmp-server host 171.71.187.101 traps version 2c private udp-port 2162</b>   | Prevents the specified host from receiving SNMPv2c traps on the configured UDP port using SNMPv2c community string (private).   |
| Step 3 | switch(config)# <b>snmp-server host 171.71.187.101 informs version 2c private udp-port 1163</b>    | Configures the specified host to receive SNMPv2c informs using SNMPv2c community string (private).                              |
|        | switch(config)# <b>no snmp-server host 171.71.187.101 informs version 2c private udp-port 2162</b> | Prevents the specified host from receiving SNMPv2c informs on the configured UDP port using SNMPv2c community string (private). |

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

To configure SNMPv2c notifications using IPv6, follow these steps:

|               | Command                                                                                                      | Purpose                                                                                                                         |
|---------------|--------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>config t</b><br>switch(config)#                                                                   | Enters configuration mode.                                                                                                      |
| <b>Step 2</b> | switch(config)# <b>snmp-server host 2001:0DB8:800:200C::417A traps version 2c private udp-port 1163</b>      | Configures the specified host to receive SNMPv2c traps using SNMPv2c community string (private).                                |
|               | switch(config)# <b>no snmp-server host 2001:0DB8:800:200C::417A traps version 2c private udp-port 2162</b>   | Prevents the specified host from receiving SNMPv2c traps on the configured UDP port using SNMPv2c community string (private).   |
| <b>Step 3</b> | switch(config)# <b>snmp-server host 2001:0DB8:800:200C::417A informs version 2c private udp-port 1163</b>    | Configures the specified host to receive SNMPv2c informs using SNMPv2c community string (private).                              |
|               | switch(config)# <b>no snmp-server host 2001:0DB8:800:200C::417A informs version 2c private udp-port 2162</b> | Prevents the specified host from receiving SNMPv2c informs on the configured UDP port using SNMPv2c community string (private). |



**Note**

Switches can forward events (SNMP traps and informs) up to 10 destinations.

## Configuring SNMPv3 Notifications

To configure SNMPv3 notifications using IPv4, follow these steps:

|               | Command                                                                                                 | Purpose                                                                                                               |
|---------------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | switch# <b>config t</b><br>switch(config)#                                                              | Enters configuration mode.                                                                                            |
| <b>Step 2</b> | switch(config)# <b>snmp-server host 16.20.11.14 traps version 3 noauth testuser udp-port 1163</b>       | Configures the specified host to receive SNMPv3 traps using SNMPv3 user (testuser) and securityLevel of noAuthNoPriv. |
|               | switch(config)# <b>snmp-server host 16.20.11.14 informs version 3 auth testuser udp-port 1163</b>       | Configures the specified host to receive SNMPv3 informs using SNMPv3 user (testuser) and securityLevel of AuthNoPriv. |
|               | switch(config)# <b>snmp-server host 16.20.11.14 informs version 3 priv testuser udp-port 1163</b>       | Configures the specified host to receive SNMPv3 informs using SNMPv3 user (testuser) and securityLevel of AuthPriv.   |
|               | switch(config)# <b>no snmp-server host 172.18.2.247 informs version 3 testuser noauth udp-port 2162</b> | Prevents the specified host from receiving SNMPv3 informs.                                                            |

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

To configure SNMPv3 notifications using IPv6, follow these steps:

|        | Command                                                                                                             | Purpose                                                                                                               |
|--------|---------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| Step 1 | switch# <b>config t</b><br>switch(config)#                                                                          | Enters configuration mode.                                                                                            |
| Step 2 | switch(config)# <b>snmp-server host 2001:0DB8:800:200C::417A traps version 3 noauth testuser udp-port 1163</b>      | Configures the specified host to receive SNMPv3 traps using SNMPv3 user (testuser) and securityLevel of noAuthNoPriv. |
|        | switch(config)# <b>snmp-server host 2001:0DB8:800:200C::417A informs version 3 auth testuser udp-port 1163</b>      | Configures the specified host to receive SNMPv3 informs using SNMPv3 user (testuser) and securityLevel of AuthNoPriv. |
|        | switch(config)# <b>snmp-server host 2001:0DB8:800:200C::417A informs version 3 priv testuser udp-port 1163</b>      | Configures the specified host to receive SNMPv3 informs using SNMPv3 user (testuser) and securityLevel of AuthPriv.   |
|        | switch(config)# <b>no snmp-server host 2001:0DB8:800:200C::417A informs version 3 testuser noauth udp-port 2162</b> | Prevents the specified host from receiving SNMPv3 informs.                                                            |

## Enabling SNMP Notifications

Notifications (traps and informs) are system alerts that the switch generates when certain events occur. You can enable or disable notifications. By default, no notification is defined or issued. If a notification name is not specified, all notifications are disabled or enabled.

With the SNMP central infra feature, you can add the traps that need to be enabled or disabled. The MIB CISCO-NOTIFICATION-CONTROL-MIB is supported to enable the use of a MIB browser to control notification generation.

You can enable or disable the supported traps at the following levels:

- Switch level—You can use **snmp-server enable traps** command to enable all the traps in the supported MIBs at the switch level.
- Feature level—You can use **snmp-server enable traps** command with the feature name to enable traps at the feature level.

```
switch =>snmp-server enable traps callhome ?
event-notify    Callhome External Event Notification
smtp-send-fail  SMTP Message Send Fail notification
```

- Individual traps - You can use **snmp-server enable traps** command with the feature name to enable traps at the individual level.

```
switch =>snmp-server enable traps callhome event-notify ?
```

Table 7-1 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 how you configured SNMP. See the notifications displayed with the **snmp-server host** CLI command.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

**Table 7-1 Enabling SNMP Notifications**

| MIB                           | Fabric Manager Check boxes                                                                                                                                                             |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CISCO-ENTITY-FRU-CONTROL-MIB  | Select the <b>Other</b> tab and check <b>FRU Changes</b> .                                                                                                                             |
| CISCO-FCC-MIB                 | Select the <b>Other</b> tab and check <b>FCC</b> .                                                                                                                                     |
| CISCO-DM-MIB                  | Select the <b>FC</b> tab and check <b>Domain Mgr RCF</b> .                                                                                                                             |
| CISCO-NS-MIB                  | Select the <b>FC</b> tab and check <b>Name Server</b> .                                                                                                                                |
| CISCO-FCS-MIB                 | Select the <b>Other</b> tab and check <b>FCS Rejects</b> .                                                                                                                             |
| CISCO-FDMI-MIB                | Select the <b>Other</b> tab and check <b>FDMI</b> .                                                                                                                                    |
| CISCO-FSPF-MIB                | Select the <b>FC</b> tab and check <b>FSPF Neighbor Change</b> .                                                                                                                       |
| CISCO-LICENSE-MGR-MIB         | Select the <b>Other</b> tab and check <b>License Manager</b> .                                                                                                                         |
| CISCO-IPSEC-SIGNALING-MIB     | Select the <b>Other</b> tab and check <b>IPSEC</b> .                                                                                                                                   |
| CISCO-PSM-MIB                 | Select the <b>Other</b> tab and check <b>Port Security</b> .                                                                                                                           |
| CISCO-RSCN-MIB                | Select the <b>FC</b> tab and check <b>RSCN ILS</b> , and <b>RCSN ELS</b> .                                                                                                             |
| SNMPv2-MIB                    | Select the <b>Other</b> tab and check <b>SNMP AuthFailure</b> .                                                                                                                        |
| VRRP-MIB, CISCO-IETF-VRRP-MIB | Select the <b>Other</b> tab and check <b>VRRP</b> .                                                                                                                                    |
| CISCO-ZS-MIB                  | Select the <b>FC</b> tab and check <b>Zone Rejects</b> , <b>Zone Merge Failures</b> , <b>Zone Merge Successes</b> , <b>Zone Default Policy Change</b> , and <b>Zone Unsuppd Mode</b> . |

The following notifications are enabled by default:

- entity fru
- license
- link ietf-extended

All other notifications are disabled by default.

To enable individual notifications, follow these steps:

|        | Command                                                  | Purpose                                                                                                            |
|--------|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Step 1 | switch# <b>config t</b><br>switch(config)#               | Enters configuration mode.                                                                                         |
| Step 2 | switch(config)# <b>snmp-server enable traps fcdomain</b> | Enables the specified SNMP (fcdomain) notification.                                                                |
|        | switch(config)# <b>no snmp-server enable traps</b>       | Disables the specified SNMP notification. If a notification name is not specified, all notifications are disabled. |

You can use the **show snmp trap** command to display all the notifications and their status.

```
switch# show snmp trap
```

```
-----
Trap type                                     Enabled
-----
entity           : entity_mib_change           Yes
entity           : entity_module_status_change Yes
```

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

|                 |                                 |     |
|-----------------|---------------------------------|-----|
| entity          | : entity_power_status_change    | Yes |
| entity          | : entity_module_inserted        | Yes |
| entity          | : entity_module_removed         | Yes |
| entity          | : entity_unrecognised_module    | Yes |
| entity          | : entity_fan_status_change      | Yes |
| entity          | : entity_power_out_change       | Yes |
| link            | : linkDown                      | Yes |
| link            | : linkUp                        | Yes |
| link            | : extended-linkDown             | Yes |
| link            | : extended-linkUp               | Yes |
| link            | : cieLinkDown                   | Yes |
| link            | : cieLinkUp                     | Yes |
| link            | : connUnitPortStatusChange      | Yes |
| link            | : fcTrunkIfUpNotify             | Yes |
| link            | : fcTrunkIfDownNotify           | Yes |
| link            | : delayed-link-state-change     | Yes |
| link            | : fcot-inserted                 | Yes |
| link            | : fcot-removed                  | Yes |
| callhome        | : event-notify                  | No  |
| callhome        | : smtp-send-fail                | No  |
| cfs             | : state-change-notif            | No  |
| cfs             | : merge-failure                 | No  |
| fcdomain        | : dmNewPrincipalSwitchNotify    | No  |
| fcdomain        | : dmDomainIdNotAssignedNotify   | No  |
| fcdomain        | : dmFabricChangeNotify          | No  |
| rf              | : redundancy_framework          | Yes |
| aaa             | : server-state-change           | No  |
| license         | : notify-license-expiry         | Yes |
| license         | : notify-no-license-for-feature | Yes |
| license         | : notify-licensefile-missing    | Yes |
| license         | : notify-license-expiry-warning | Yes |
| scsi            | : scsi-disc-complete            | No  |
| fcns            | : reject-reg-req                | No  |
| fcns            | : local-entry-change            | No  |
| fcns            | : db-full                       | No  |
| fcns            | : remote-entry-change           | No  |
| rscn            | : rscnElsRejectReqNotify        | No  |
| rscn            | : rscnIlsRejectReqNotify        | No  |
| rscn            | : rscnElsRxRejectReqNotify      | No  |
| rscn            | : rscnIlsRxRejectReqNotify      | No  |
| fcs             | : request-reject                | No  |
| fcs             | : discovery-complete            | No  |
| fctrace         | : route                         | No  |
| zone            | : request-reject1               | No  |
| zone            | : merge-success                 | No  |
| zone            | : merge-failure                 | No  |
| zone            | : default-zone-behavior-change  | No  |
| zone            | : unsupp-mem                    | No  |
| port-security   | : fport-violation               | No  |
| port-security   | : eport-violation               | No  |
| port-security   | : fabric-binding-violation      | No  |
| vni             | : virtual-interface-created     | No  |
| vni             | : virtual-interface-removed     | No  |
| vsan            | : vsanStatusChange              | No  |
| vsan            | : vsanPortMembershipChange      | No  |
| fspf            | : fspfNbrStateChangeNotify      | No  |
| upgrade         | : UpgradeOpNotifyOnCompletion   | No  |
| upgrade         | : UpgradeJobStatusNotify        | No  |
| feature-control | : FeatureOpStatusChange         | No  |
| vrrp            | : cVrrpNotificationNewMaster    | No  |
| fdmi            | : cfdmiRejectRegNotify          | No  |
| snmp            | : authentication                | No  |

*Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)*

## Configuring the Notification Target User

You must configure a notification target user on the switch for sending SNMPv3 inform notifications to the SNMP manager.

To configure the notification target user, use the following command:

|        | Command                                                                                                                                             | Purpose                                                                                                                   |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Step 1 | switch# <b>config t</b><br>switch(config)#                                                                                                          | Enters configuration mode.                                                                                                |
| Step 2 | switch(config)# <b>snmp-server user testusr</b><br><b>auth md5 xyub20gh priv xyub20gh engineID</b><br><b>00:00:00:63:00:01:00:a1:ac:15:10:03</b>    | Configures the notification target user with the specified credentials for the SNMP manager with the specified engine ID. |
|        | switch(config)# <b>no snmp-server user testusr</b><br><b>auth md5 xyub20gh priv xyub20gh engineID</b><br><b>00:00:00:63:00:01:00:a1:ac:15:10:03</b> | Removes the notification target user.                                                                                     |

The credentials of the notification target user are used for encrypting the SNMPv3 inform notification messages to the configured SNMP manager (as in the **snmp-server host** command).



### Note

For authenticating and decrypting the received INFORM PDU, the SNMP manager should have the same user credentials in its local configuration data store of users.

## Configuring LinkUp/LinkDown Notifications for Switches

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

- Cisco—Only notifications (cieLinkUp, cieLinkDown) defined in CISCO-IF-EXTENSION-MIB.my are sent for an interface, if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface.
- IETF—Only notifications (linkUp, linkDown) defined in IF-MIB are sent for an interface, if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface. Only the varbinds defined in the notification definition are sent with the notifications.
- IETF extended—Only notifications (linkUp, linkDown) defined in IF-MIB are sent for an interface, if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface. In addition to the varbinds defined in the notification definition, varbinds defined in the IF-MIB specific to the Cisco Systems implementation are sent. This is the default setting.
- IETF Cisco—Only notifications (linkUp, linkDown) defined in IF-MIB and notifications (cieLinkUp, cieLinkDown) defined in CISCO-IF-EXTENSION-MIB.my are sent for an interface, if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface. Only the varbinds defined in the notification definition are sent with the linkUp and linkDown notifications.
- IETF extended Cisco—Only notifications (linkUp, linkDown) defined in IF-MIB and notifications (cieLinkUp, cieLinkDown) defined in CISCO-IF-EXTENSION-MIB.my are sent for an interface, if ifLinkUpDownTrapEnable (defined in IF-MIB) is enabled for that interface. In addition to the varbinds defined in linkUp and linkDown notification definition, varbinds defined in the IF-MIB specific to the Cisco Systems implementation are sent with the linkUp and linkDown notifications.

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

**Note**

For more information on the varbinds defined in the IF-MIB specific to the Cisco Systems implementation, refer to the *Cisco MDS 9000 Family MIB Quick Reference*.

To configure the linkUp/linkDown notification for a switch using NX-OS Release 4.1(x) and earlier, follow these steps:

|        | Command                                                                  | Purpose                                                                                                                           |
|--------|--------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | switch# <b>config t</b><br>switch(config)#                               | Enters configuration mode.                                                                                                        |
| Step 2 | switch(config)# <b>snmp-server enable traps link</b>                     | Enables (default) only IETF extended linkUp/linkDown notifications.                                                               |
|        | switch(config)# <b>snmp-server enable traps link cisco</b>               | Enables only Cisco Systems defined cieLinkUp/cieLinkDown notifications.                                                           |
|        | switch(config)# <b>snmp-server enable traps link ietf</b>                | Enables only IETF linkUp/linkDown notifications.                                                                                  |
|        | switch(config)# <b>snmp-server enable traps link ietf-extended</b>       | Enables (default) only IETF extended linkUp/linkDown notifications with extra varbinds.                                           |
|        | switch(config)# <b>snmp-server enable traps link ietf cisco</b>          | Enables IETF (linkUp/linkDown) and Cisco Systems defined (cieLinkUp/cieLinkDown) notifications.                                   |
|        | switch(config)# <b>snmp-server enable traps link ietf-extended cisco</b> | Enables IETF (linkUp/linkDown) notifications with extra varbinds and Cisco Systems defined (cieLinkUp/cieLinkDown) notifications. |
|        | switch(config)# <b>no snmp-server enable traps link</b>                  | Reverts to the default setting (IETF extended).                                                                                   |

**Note**

If both IETF and IETF extended are enabled, the **show snmp traps** command displays both as enabled. However, as a trap, you will receive only one trap with IETF extended payload.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

To configure the linkUp/linkDown notification for a switch using NX-OS Release 4.2(1) and later, follow these steps:

|        | Command                                                                        | Purpose                                                                  |
|--------|--------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| Step 1 | switch# <b>config t</b><br>switch(config)#                                     | Enters configuration mode.                                               |
| Step 2 | switch(config)# <b>snmp-server enable traps link extended-link</b>             | Enables only IETF extended linkUp notifications.                         |
|        | switch(config)# <b>snmp-server enable traps link extended-linkDown</b>         | Enables only IETF extended linkDown notifications.                       |
|        | switch(config)# <b>snmp-server enable traps link cieLinkDown</b>               | Enables Cisco extended link state down notification.                     |
|        | switch(config)# <b>snmp-server enable traps link cieLinkUp</b>                 | Enables Cisco extended link state up notification.                       |
|        | switch(config)# <b>snmp-server enable traps link connUnitPortStatusChange</b>  | Enables FCMGMT The overall status of the connectivity unit Notification. |
|        | switch(config)# <b>snmp-server enable traps link delayed-link-state-change</b> | Enables Delayed link state change.                                       |
|        | switch(config)# <b>snmp-server enable traps link extended-linkDown</b>         | Enables IETF extended link state down notification.                      |
|        | switch(config)# <b>snmp-server enable traps link extended-linkUp</b>           | Enables IETF extended link state down notification.                      |
|        | switch(config)# <b>snmp-server enable traps link fcTrunkIfDownNotify</b>       | Enables FCFE Link state down notification.                               |
|        | switch(config)# <b>snmp-server enable traps link fcTrunkIfUpNotify</b>         | Enables FCFE Link state up notification.                                 |
|        | switch(config)# <b>snmp-server enable traps link fcot-inserted</b>             | Enables FCOT info trap.                                                  |
|        | switch(config)# <b>snmp-server enable traps link fcot-removed</b>              | Enables FCOT info trap.                                                  |
|        | switch(config)# <b>snmp-server enable traps link linkDown</b>                  | Enables IETF Link state down notification.                               |
|        | switch(config)# <b>snmp-server enable traps link linkUp</b>                    | Enables IETF Link state up notification.                                 |
|        | switch(config)# <b>no snmp-server enable traps link</b>                        | Reverts to the default setting (IETF extended).e                         |

## Configuring Up/Down SNMP Link-State Traps for Interfaces

By default, SNMP link-state traps are enabled for all interfaces. Whenever a link toggles its state from Up to Down or vice versa, an SNMP trap is generated.

In some instances, you may find that you have numerous switches with hundreds of interfaces, many of which do not require monitoring of the link state. In such cases, you may elect to disable link-state traps.

To disable SNMP link-state traps for specific interfaces, follow these steps:

|        | Command                                    | Purpose                    |
|--------|--------------------------------------------|----------------------------|
| Step 1 | switch# <b>config t</b><br>switch(config)# | Enters configuration mode. |

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

|        | Command                                      | Purpose                                                            |
|--------|----------------------------------------------|--------------------------------------------------------------------|
| Step 2 | switch(config)# <b>interface bay 6</b>       | Specifies the interface on which to disable SNMP link-state traps. |
|        | switch(config-if)# <b>no link-state-trap</b> | Disables SNMP link-state traps for the interface.                  |
|        | switch(config-if)# <b>link-state-trap</b>    | Enables SNMP link-state traps for the interface.                   |

Whenever you disable an SNMP link-state trap for an interface, the command is also added to the running configuration of the system. To view the running configuration, enter the **show running-config** command for the interface.

```
switch# show running-config
version 3.1(2)
....
interface bay5
interface bay6
  no link-state-trap <-----command is added to the running configuration for the interface
interface bay7...
```

To view the SNMP link-state trap configuration for a particular interface, enter the **show interface** command.

```
switch# show interface bay 6
bay6 is down (Administratively down)
  Hardware is Fibre Channel
  Port WWN is 20:0b:00:05:30:01:70:2c
  Admin port mode is auto, trunk mode is on
  snmp link-state traps are disabled

  Port vsan is 1
  Receive data field Size is 2112
  Beacon is turned off
  5 minutes input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
  5 minutes output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    0 frames input, 0 bytes
      0 discards, 0 errors
      0 CRC, 0 unknown class
      0 too long, 0 too short
    0 frames output, 0 bytes
      0 discards, 0 errors
    0 input OLS, 0 LRR, 0 NOS, 0 loop inits
    0 output OLS, 0 LRR, 0 NOS, 0 loop inits
```

## Scope of Link Up/Down Trap Settings

The link Up/Down trap settings for the interfaces generate traps based on the following scope:

| Switch-level Trap Setting | Interface-level Trap Setting | Trap Generated for Interface Links? |
|---------------------------|------------------------------|-------------------------------------|
| Enabled (default)         | Enabled (default)            | Yes                                 |
| Enabled                   | Disabled                     | No                                  |
| Disabled                  | Enabled                      | No                                  |
| Disabled                  | Disabled                     | No                                  |

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

## Configuring Entity (FRU) Traps

To enable individual SNMP trap control, follow these steps:

|        | Command                                                               | Purpose                               |
|--------|-----------------------------------------------------------------------|---------------------------------------|
| Step 1 | switch# <b>config t</b><br>switch(config)#                            | Enters configuration mode.            |
| Step 2 | switch(config)# <b>snmp-server enable traps entity</b>                | Enables individual SNMP trap control. |
|        | switch(config)# <b>snmp-server enable entity_fan_status_change</b>    | Enables entity fan status change.     |
|        | switch(config)# <b>snmp-server enable entity_mib_change</b>           | Enables entity MIB change.            |
|        | switch(config)# <b>snmp-server enable entity_module_inserted</b>      | Enables entity module to be inserted. |
|        | switch(config)# <b>snmp-server enable entity_module_removed</b>       | Enables entity module to be removed.  |
|        | switch(config)# <b>snmp-server enable entity_module_status_change</b> | Enables entity module status change.  |
|        | switch(config)# <b>snmp-server enable entity_power_out_change</b>     | Enables entity power out change.      |
|        | switch(config)# <b>snmp-server enable entity_power_status_change</b>  | Enables entity power status change.   |
|        | switch(config)# <b>snmp-server enable entity_unrecognised_module</b>  | Enables entity unrecognised module.   |



### Note

All these traps have to do with legacy FRU traps.

## Displaying SNMP Security Information

Use the **show snmp** commands to display configured SNMP information (see [Example 7-1](#) and [7-6](#)).

### Example 7-1 Displays SNMP User Details

```
switch# show snmp user
```

```

SNMP USERS

User                               Auth  Priv(enforce)  Groups
-----
admin                               md5    des(no)         network-admin

testusr                             md5    aes-128(no)    role111
                                         role222

NOTIFICATION TARGET USERS (configured for sending V3 Inform)

User                               Auth  Priv
-----
testtargetusr                       md5    des
(EngineID 0:0:0:63:0:1:0:0:0:15:10:3)
```

**Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)**

### Example 7-2 Displays SNMP Community Information

```
switch# show snmp community
Community                Access
-----                -
private                  rw
public                   ro
v93RACqPNH               ro
```

### Example 7-3 Displays SNMP Host Information

```
switch# show snmp host
Host                      Port Version Level Type SecName
-----
171.16.126.34            2162 v2c    noauth trap public
171.16.75.106            2162 v2c    noauth trap public
...
171.31.58.97             2162 v2c    auth  trap public
...
```

The **show snmp** command displays counter information for SNMP contact, location, and packet settings. This command provides information that is used entirely by the Cisco MDS 9000 Family Fabric Manager (refer to the *Cisco Fabric Manager System Management Configuration Guide*). See [Example 7-4](#).

### Example 7-4 Displays SNMP Information

```
switch# show snmp
sys contact:
sys location:
1631 SNMP packets input
    0 Bad SNMP versions
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    64294 Number of requested variables
    1 Number of altered variables
    1628 Get-request PDUs
    0 Get-next PDUs
    1 Set-request PDUs
152725 SNMP packets output
    0 Too big errors
    1 No such name errors
    0 Bad values errors
    0 General errors

Community                Group / Access
-----                -
public                   rw
```

---

SNMP USERS

---

| User    | Auth | Priv(enforce) | Groups             |
|---------|------|---------------|--------------------|
| admin   | md5  | des(no)       | network-admin      |
| testusr | md5  | aes-128(no)   | role111<br>role222 |

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

---

NOTIFICATION TARGET USERS (configured for sending V3 Inform)

---

| User                                  | Auth | Priv |
|---------------------------------------|------|------|
| testtargetusr                         | md5  | des  |
| (EngineID 0:0:0:63:0:1:0:0:0:15:10:3) |      |      |

#### **Example 7-5 Displays SNMP Engine IDs**

```
switch# show snmp engineID
Local SNMP engineID: [Hex] 8000000903000DEC2CF180
                    [Dec] 128:000:000:009:003:000:013:236:044:241:128
```

#### **Example 7-6 Displays Information on SNMP Security Groups**

```
switch# show snmp group
groupname: network-admin
security model: any
security level: noAuthNoPriv
readview: network-admin-rd
writeview: network-admin-wr
notifyview: network-admin-rd
storage-type: permanent
row status: active

groupname: network-admin
security model: any
security level: authNoPriv
readview: network-admin-rd
writeview: network-admin-wr
notifyview: network-admin-rd
storage-type: permanent
row status: active

groupname: network-operator
security model: any
security level: noAuthNoPriv
readview: network-operator-rd
writeview: network-operator-wr
notifyview: network-operator-rd
storage-type: permanent
row status: active

groupname: network-operator
security model: any
security level: authNoPriv
readview: network-operator-rd
writeview: network-operator-wr
notifyview: network-operator-rd
storage-type: permanent
row status: active
```

## Default Settings

Table 7-2 lists the default settings for all SNMP features in any switch.

***Send documentation comments to [mdsfeedback-doc@cisco.com](mailto:mdsfeedback-doc@cisco.com)***

**Table 7-2**      **Default SNMP Settings**

| Parameters   | Default                       |
|--------------|-------------------------------|
| User account | No expiry (unless configured) |
| Password     | None                          |