CHAPTER 14

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.

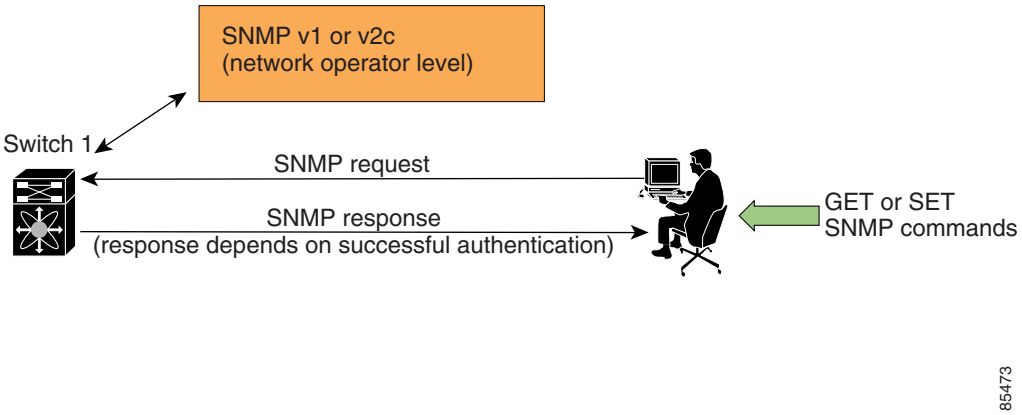
Users, passwords, and roles for all CLI and SNMP users are the same. A user configured through the CLI can access the switch using SNMP (for example, the DCNM-SAN or the Device Manager) and vice versa.

This chapter includes the following sections:

Information 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 14-1).

Figure 14-1 SNMP Security



This section includes the following topics:

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.

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.

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.

Note Starting in 3.0(1), the temporary SNMP login created for DCNM-SAN is no longer 24 hours. It is one hour.

- 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).

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, DCNM-SAN, 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.
- DCNM-SAN.
- 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 (DCNM-SAN 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 DCNM-SAN or Device Manager. However, after you use the CLI password to log into DCNM-SAN 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.

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.

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.

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.

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.
- IEFT 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.
- IEFT 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.
- IEFT 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.

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.*

Scope of LinkUp and LinkDown Trap Settings

The LinkUp and LinkDown 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 (defualt)	Enabled (default)	Yes
Enabled	Disabled	No

Switch-level Trap Setting	Interface-level Trap Setting	Trap Generated for Interface Links?
Disabled	Enabled	No
Disabled	Disabled	No

Default Settings

Table 14-1 lists the default settings for all SNMP features in any switch.

Table 14-1 Default SNMP Settings

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

Configuring SNMP

SNMP is an application layer protocol that facilitates the exchange of management information between network devices.

This section includes the following topics:

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# config t`	Enters configuration mode.
Step 2	`switch(config)# snmp-server contact NewUser`	Assigns the contact name for the switch.
	`switch(config)# no snmp-server contact NewUser`	Deletes the contact name for the switch.
Step 3	`switch(config)# snmp-server location SanJose`	Assigns the switch location.
	`switch(config)# no snmp-server location SanJose`	Deletes the switch location.

To configure contact and location information, follow these steps:

Step 1 Expand **Switches** from the Physical Attributes pane.

You see the switch settings in the Information pane.

Step 2 Fill in the Location and Contact fields for each switch.

Step 3 Click **Apply Changes** to save these changes or click **Undo Changes** to discard any unsaved changes.

Configuring SNMP Users from the CLI

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

Restrictions

- 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.

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

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# snmp-server user joe network-admin auth sha abcd1234`	Creates or modifies the settings for a user (joe) in the network-admin role using the HMAC-SHA-96 authentication password (abcd1234).
	`switch(config)# snmp-server user sam network-admin auth md5 abcdefgh`	Creates or modifies the settings for a user (sam) in the network-admin role using the HMAC-MD5-96 authentication password (abcdefgh).
	`switch(config)# snmp-server user Bill network-admin auth sha abcd1234 priv abcdefgh`	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)# no snmp-server user usernameA`	Deletes the user (usernameA) and all associated parameters.
	`switch(config)# no snmp-server usam role vsan-admin`	Deletes the specified user (usam) from the vsan-admin role.

	Command	Purpose
	`switch(config)# snmp-server user user1 network-admin auth md5 0xab0211gh priv 0x45abf342 localizedkey`	Specifies the password to be in localized key format (RFC 2574). The localized key is provided in hexadecimal format (for example, 0xacbdef).
	`switch(config)# snmp-server user user2 auth md5 asdgfsadf priv aes-128 asgfsgkhkj`	Configures the user2 with the MD5 authentication protocol and AES-128 privacy protocol.
Step 3	`switch(config)# snmp-server user joe sangroup`	Adds the specified user (joe) to the sangroup role.
	`switch(config)# snmp-server user joe techdocs`	Adds the specified user (joe) to the techdocs role.

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

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

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 14-17). 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.

Note Either to create a new SNMPv3 user or modify password of SNMPv3 user, the DCNM login user need to have enabled with DES/AES privacy password. Since the creating and modifying SNMP SET request need to be encrypted, the login user password needs to have the privacy password.

Detailed Steps

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

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# snmp-server user testUser enforcePriv`	Enforces the message encryption for SNMPv3 messages using this user. **Note** 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)# no snmp-server user testUser enforcePriv`	Disables SNMPv3 message encryption enforcement.

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

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

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

Step 1 Expand **Switches,** expand **Security,** and then select **Users and Roles** from the Physical Attributes pane.

Step 2 Click the **Users** tab in the Information pane to see a list of users.

Step 3 Click **Create Row**.

You see the Create Users dialog box.

Step 4 Enter the user name in the **New User** field.

Step 5 Select the role from the Role drop-down menu. You can enter a new role name in the field if you do not want to select one from the drop-down menu. If you do this, you must go back and configure this role appropriately.

Step 6 Enter a password for the user in Password field.

Step 7 Click the **Privacy** tab.

Step 8 Check the **Enforce SNMP Privacy Encryption** check box to encrypt management traffic.

Step 9 Click **Create** to create the new entry.

To enforce the SNMPv3 message encryption globally on all the users, follow these steps:

Step 1 Select a VSAN in the Logical Domains pane. This will not work if you select All VSANS.

Step 2 Expand **Switches,** expand **Security,** and then select **Users and Roles** in the Physical Attributes pane. Click the **Global** tab in the Information pane.

Step 3 Check the **GlobalEnforcePriv** check box.

Step 4 Click the **Apply Changes** icon to save these changes.

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.

Restrictions

- 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# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# snmp-server user NewUser role1`	Creates or modifies the settings for an SNMPv3 user (NewUser) for the role1 role.
	`switch(config)# snmp-server user NewUser role2`	Creates or modifies the settings for an SNMPv3 user (NewUser) for the role2 role.
	`switch(config)# no snmp-server user User5 role2`	Removes role2 for the specified user (User5).

To add multiple roles to a new user, follow these steps:

Step 1 Expand **Switches,** expand **Security,** and then select **Users and Roles** from the Physical Attributes pane.

Step 2 Click the **Users** tab in the Information pane to see a list of users.

Step 3 Click **Create Row**.

You see the Create Users dialog box.

Step 4 Choose roles using the check boxes.

Step 5 Choose an option for Digest and one for Encryption.

Step 6 (Optional) Provide an expiration date for the user and the file name of an SSH key.

Step 7 Click **Create** to create the new roles.

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# config t`	Enters configuration mode.
Step 2	`switch(config)# snmp-server community snmp_Community ro`	Adds read-only access for the specified SNMP community.
	`switch(config)# snmp-server community snmp_Community rw`	Adds read-write access for the specified SNMP community.
	`switch(config)# no snmp-server community snmp_Community`	Deletes access for the specified SNMP community (default).

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

Step 1 Expand **Switches,** expand **Security,** and then select **Users and Roles** from the Physical Attributes pane.

Step 2 Click the **Communities** tab in the Information pane.

You see the existing communities.

Step 3 Click **Create Row**.

You see the Create Community String dialog box.

Step 4 Check the **Switch** check boxes to specify one or more switches.

Step 5 Enter the community name in the Community field.

Step 6 Select the role from Role drop-down list.

Note You can enter a new role name in the field if you do not want to select one from the drop-down list. If you do this, you must go back and configure this role appropriately.

Step 7 Click **Create** to create the new entry.

Deleting a Community String

To delete a community string, follow these steps:

Step 1 Expand **Switches,** expand **Security,** and then select **Users and Roles** from the Physical Attributes pane.

Step 2 Click the **Communities** tab in the Information pane.

Step 3 Click the name of the community you want to delete.

Step 4 Click **Delete Row** to delete this community.

Configuring SNMP Trap and Inform Notifications

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

Note You must enable the RMON traps in the SNMP configuration. For more information, refer to "Configuring RMON" section on page 53-1.

Note 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:

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# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# snmp-server host 171.71.187.101 traps version 2c private udp-port 1163`	Configures the specified host to receive SNMPv2c traps using SNMPv2c community string (private).
	`switch(config)# no snmp-server host 171.71.187.101 traps version 2c private udp-port 2162`	Prevents the specified host from receiving SNMPv2c traps on the configured UDP port using SNMPv2c community string (private).

	Command	Purpose
Step 3	`switch(config)# snmp-server host 171.71.187.101 informs version 2c private udp-port 1163`	Configures the specified host to receive SNMPv2c informs using SNMPv2c community string (private).
	`switch(config)# no snmp-server host 171.71.187.101 informs version 2c private udp-port 2162`	Prevents the specified host from receiving SNMPv2c informs on the configured UDP port using SNMPv2c community string (private).

To configure SNMPv2c notifications using IPv6, follow these steps:

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

To configure SNMPv2c notifications, follow these steps:

Step 1 Expand **Events** and then select **SNMP Traps** in the Physical Attributes pane.

You see the SNMP notification configuration in the Information pane.

Step 2 Click the **Destinations** tab to add or modify a receiver for SNMP notifications.

Step 3 Click **Create Row** to create a new notification destination.

You see the Create Destinations dialog box.

Step 4 Check the switches for which you want to configure a new destination.

Step 5 Set the destination IP address and UDP port.

Step 6 Choose either the **trap** or **inform** radio button.

Step 7 (Optional) Set the timeout or retry count values.

Step 8 Click **Create** to add this destination to the selected switches.

Step 9 (Optional) Click the **Other** tab to enable specific notification types per switch.

Step 10 Click the **Apply changes** icon to create the entry.

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

To configure SNMPv3 notifications using IPv6, follow these steps:

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

To configure SNMPv3 notifications, follow these steps:

Step 1 Select **v3** from the **Security** drop-down list in the **Create Destinations** dialog box.

Step 2 (Optional) Set the inform time out and retry values.

Step 3 Click **Create** to add this destination to the selected switches.

Note In the case of SNMPv3 notifications, the SNMP manager is expected to know the user credentials (authKey/PrivKey) based on the switch's engineID to authenticate and decrypt the SNMP messages.

Enabling SNMP Notifications

Table 14-2 lists the CLI commands that enable the notifications for Cisco NX-OS MIBs.

Table 14-2 lists the DCNM-SAN procedures that enable the notifications for Cisco NX-OS MIBs.

Expand **Events > SNMP Traps** to see the check boxes listed in this table.

Note Choosing **Events > SNMP Traps** enables both traps and informs, depending on how you configured SNMP notifications. See the notifications displayed with the "Configuring SNMPv3 Notifications" section on page 14-14.

Table 14-2 Enabling SNMP Notifications

MIB	DCNM-SAN Check Boxes
CISCO-ENTITY-FRU-CONTROL-MIB	Click the **Other** tab and check **FRU Changes**.
CISCO-FCC-MIB	Click the **Other** tab and check **FCC**.
CISCO-DM-MIB	Click the **FC** tab and check **Domain Mgr RCF**.
CISCO-NS-MIB	Click the **FC** tab and check **Name Server**.
CISCO-FCS-MIB	Click the **Other** tab and check **FCS Rejects**.
CISCO-FDMI-MIB	Click the **Other** tab and check **FDMI**.
CISCO-FSPF-MIB	Click the **FC** tab and check **FSPF Neighbor Change**.
CISCO-LICENSE-MGR-MIB	Click the **Other** tab and check **License Manager**.
CISCO-IPSEC-SIGNALLING-MIB	Click the **Other** tab and check **IPSEC**.
CISCO-PSM-MIB	Click the **Other** tab and check **Port Security**.
CISCO-RSCN-MIB	Click the **FC** tab and check **RSCN ILS**, and **RCSN ELS**.
SNMPv2-MIB	Click the **Other** tab and check **SNMP AuthFailure**.
VRRP-MIB, CISCO-IETF-VRRP-MIB	Click the **Other** tab and check **VRRP.**
CISCO-ZS-MIB	Click the **FC** tab and check **Zone Rejects**, **Zone Merge Failures**, **Zone Merge Successes**, **Zone Default Policy Change**, and **Zone Unsuppd Mode**.

The following notifications are enabled by default:

- entity fru

- license
- link ietf-extended

All other notifications are disabled by default.

Summary Steps

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 ?
```

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.

To enable individual notifications, follow these steps:

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

To enable individual notifications, follow these steps:

Step 1 Expand **Events** and then select **SNMP Traps** in the Physical Attributes pane.

You see the SNMP notification configuration in the Information pane.

Step 2 Click the **FC** tab to enable Fibre Channel related notifications.

Step 3 Check each notification check box that you want to enable.

Step 4 Click the **Other** tab to enable other notifications.

Step 5 Check each notification check box that you want to enable.

Step 6 Click the **Control** tab to enable notification applicable variables.

Step 7 From NX-OS Release 4.2(1), the **Control** tab is available for the notification control feature. This feature allows you to enable or disable all the notification-applicable variables via SNMP.

The **Control** tab is available for NX-OS Release 4.2(1) and later only.

Step 8 Check each notification check box that you want to enable.

Step 9 Click the **Apply changes** icon to create the entry.

Note In Device Manager, the **no snmp-server enable traps link** command disables generation of link traps in the switch, however the individual interfaces may have the link trap enabled.

To enable individual notifications using Device Manager, follow these steps:

Step 1 Expand **Admin > Events** and then select **Filters**.

You see the event filters window showing a table populated by the switch

Step 2 Click the **Control** tab to enable notification applicable variables.

From NX-OS Release 4.2(1), the **Control** tab is available for the notification control feature. This feature allows you to enable or disable all the notification-applicable variables via SNMP.

Note The **Control** tab is available for NX-OS Release 4.2(1) and later only.

Step 3 Check each notification check box that you want to enable.

Step 4 Click the **Apply changes** icon to create the entry.

Configuring the Notification Target User

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

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.

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

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

To configure the notification target user, refer to the *Cisco MDS 9000 Family NX-OS System Management Configuration Guide*.

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

Configuring LinkUp/LinkDown Notifications for Switches

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# config t` `switch(config)#`	Enters configuration mode.
Step 1	`switch(config)# snmp-server enable traps link`	Enables (default) only IETF extended LinkUp/LinkDown notifications.
	`switch(config)# snmp-server enable traps link cisco`	Enables only Cisco Systems defined cieLinkUp/cieLinkDown notifications.
	`switch(config)# snmp-server enable traps link ietf`	Enables only IETF LinkUp/LinkDown notifications.
	`switch(config)# snmp-server enable traps link ietf-extended`	Enables (default) only IETF extended LinkUp/LinkDown notifications with extra varbinds.
	`switch(config)# snmp-server enable traps link ietf cisco`	Enables IETF (LinkUp/LinkDown) and Cisco Systems defined (cieLinkUp/cieLinkDown) notifications.
	`switch(config)# snmp-server enable traps link ietf-extended cisco`	Enables IEFT (LinkUp/LinkDown) notifications with extra varbinds and Cisco Systems defined (cieLinkUp/cieLinkDown) notifications.
	`switch(config)# no snmp-server enable traps link`	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.

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

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# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# interface bay 6`	Specifies the interface on which to disable SNMP link-state traps.
	`switch(config-if)# no link-state-trap`	Disables SNMP link-state traps for the interface.
	`switch(config-if)# link-state-trap`	Enables SNMP link-state traps for the interface.

Configuring Entity (FRU) Traps

To enable individual SNMP trap control, follow these steps:

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

Note All these traps have to do with legacy FRU traps.

Configuring Event Security

SNMP events can be secured against interception or eavesdropping in the same way that SNMP messages are secured. DCNM-SAN or Device Manager allow you to configure the message processing model, the security model, and the security level for the SNMP events that the switch generates.

Restrictions

- This is an advanced function that should only be used by administrators having experience with SNMPv3.

To configure SNMP event security, follow these steps:

Step 1 Expand **Events** and then select **SNMP Traps.**

Step 2 Click the **Security** tab in the Information pane.

You see the security information for SNMP notifications.

Step 3 Set the message protocol model (MPModel), security model, security name, and security level.

Step 4 Click the **Apply Changes** icon to save and apply your changes.

Viewing the SNMP Events Log

Prerequisites

- You must set up the MDS syslog manager before you can view the event logs.

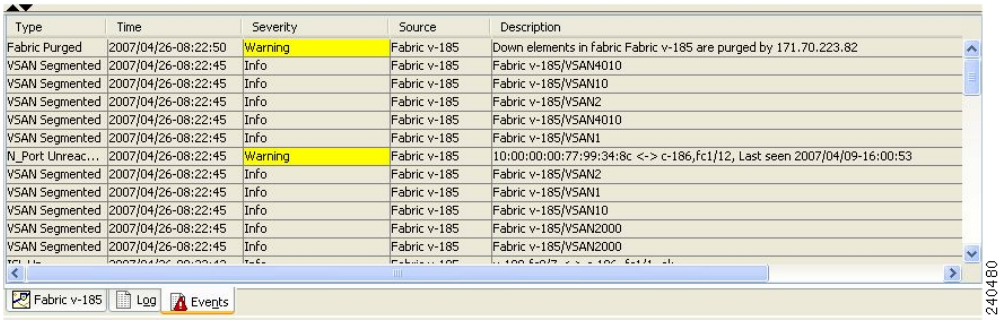
Restrictions

- Changing these values from different DCNM-SAN workstations at the same time may cause unpredictable results.

Step 1 To view the SNMP events log from DCNM-SAN, click the **Events** tab.

You see the Events listed with a log of events for a single switch (see Figure 14-2).

Figure 14-2 Events Information



Verifying SNMP Configuration

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

Command	Purpose
show running-config	Displays the running configuration
show interface	Displays the SNMP link-state trap configuration for a particular interface
show snmp trap	Displays all the notifications and their status
show snmp	Displays configured SNMP informatio, counter information for SNMP contact, location, and packet settings.

For detailed information about the fields in the output from these commands, refer to the *Cisco MDS 9000 Family Command Reference*.

This section covers the following topics:

- Viewing the Up/Down SNMP Link-State Traps for Interfaces section, page 14-22
- Displaying SNMP Traps section, page 14-23
- Displaying SNMP Security Information section, page 14-24

Viewing the Up/Down SNMP Link-State Traps for Interfaces

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, use 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
```

Displaying SNMP Traps

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
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
```

Displaying SNMP Security Information

Use the **show snmp** commands to display configured SNMP information (see Example 14-1 and 14-6).

Example 14-1 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)
```

Example 14-2 Displays SNMP Community Information

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

Example 14-3 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 DCNM-SAN (refer to the *System Management Configuration Guide, Cisco DCNM for SAN*). See Example 14-4.

Example 14-4 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
                                                    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)
```

Example 14-5 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 14-6 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
```

Field Descriptions for SNMP

This section describes the field descriptions for SNMP.

IP Statistics SNMP

Field	Description
BadVersions	The total number of SNMP messages which were delivered to the SNMP entity and were for an unsupported SNMP version.
BadCommunityNames	The total number of SNMP messages delivered to the SNMP entity which used a SNMP community name not known to said entity.
BadCommunityUses	The total number of SNMP messages delivered to the SNMP entity which represented an SNMP operation which was not allowed by the SNMP community named in the message.
ASNParseErrs	The total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.

Field	Description
TooBigs	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is tooBig.
SilentDrops	The total number of GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMP entity which were silently dropped because the size of a reply containing an alternate Response-PDU with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request.
ProxyDrops	The total number of GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMP entity which were silently dropped because the transmission of the (possibly translated) message to a proxy target failed in a manner (other than a time-out) such that no Response-PDU could be returned.
NoSuchNames	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is noSuchName.
BadValues	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is badValue.
ReadOnlys	The total number valid SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is readOnly. It should be noted that it is a protocol error to generate an SNMP PDU which contains the value readOnly in the error-status field, as such this is provided as a means of detecting incorrect implementations of the SNMP.
GenErrs	The total number of SNMP PDUs which were delivered to the SNMP protocol entity and for which the value of the error-status field is genErr.
Pkts	The total number of messages delivered to the SNMP entity from the transport service.
GetRequests	The total number of SNMP Get-Request PDUs which have been accepted and processed by the SNMP protocol entity.
GetNexts	The total number of SNMP Get-Next PDUs which have been accepted and processed by the SNMP protocol entity.
SetRequests	The total number of SNMP Set-Request PDUs which have been accepted and processed by the SNMP protocol entity.
OutTraps	The total number of SNMP Trap PDUs which have been generated by the SNMP protocol entity.
OutGetResponses	The total number of SNMP Get-Response PDUs which have been generated by the SNMP protocol entity.
OutPkts	The total number of SNMP Messages which were passed from the SNMP protocol entity to the transport service.

Field	Description
TotalReqVars	The total number of MIB objects which have been retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
TotalSetVars	The total number of MIB objects which have been altered successfully by the SNMP protocol entity as the result of receiving valid SNMP Set-Request PDUs.

SNMP Security Users

Field	Description
Role	The user in Security Model independent format.
Password	Password of the common user. For SNMP, this password is used for both authentication and privacy. For CLI and XML, it is used for authentication only.
Digest	The type of digest authentication protocol which is used.
Encryption	The type of encryption authentication protocol which is used.
ExpiryDate	The date on which this user will expire.
SSH Key File Configured	Specifies whether the user is configured with SSH public key.
SSH Key File	The name of the file storing the SSH public key. The SSH public key is used to authenticate the SSH session for this user. Note that this applies to only CLI user. The format can be one of the following: • SSH Public Key in OpenSSH format • SSH Public Key in IETF SECSH (Commercial SSH public key format) • SSH Client Certificate in PEM (privacy-enhanced mail format) from which the public key is extracted • SSH Client Certificate DN (Distinguished Name) for certificate based authentication
Creation Type	The type of the credential store of the user. When a row is created in this table by a user, the user entry is created in a credential store local to the device. In case of remote authentication mechanism like AAA Server based authentication, credentials are stored in other (remote) system/device.
Expiry Date	The date on which this user will expire.

Related Topics

Configuring SNMP

SNMP Security Communities

Field	Description
Community	The community string.
Role	The Security Model name.

Related Topics

Adding or Deleting Communities

Deleting a Community String

Security Users Global

Field	Description
Enforce SNMP Privacy Encryption	Specifies whether the SNMP agent enforces the use of encryption for SNMPv3 messages globally on all the users in the system.
Cache Timeout	This specifies maximum timeout value for caching the user credentials in the local system.

Note The privacy password and authentication password are required for an administrator to create a new user or delete an existing user in Device Manager. However, if the administrator does not provide these credentials at the time of creating a new user, Device Manager uses the authentication password of the administrator as the privacy password. If the privacy protocol defined for the user is not DES (default), the SNMP Agent in the MDS will not be able to decrypt the packet and the SNMP Agent times out. If the privacy protocol defined for the user is not DES, the user needs to provide both the privacy password and the protocol when logging in.

Additional References

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

- MIBs section, page 14-29

MIBs

MIBs	MIBs Link
• CISCO-SNMP-TARGET-EXT-MIB • CISCO-SNMP-VACM-EXT-MIB	To locate and download MIBs, go to the following URL: http://www.cisco.com/en/US/products/ps5989/prod_technical_reference_list.html

Feature History for SNMP

Table 14-3 lists the release history for this feature. Only features that were introduced or modified in Release 3.x or a later release appear in the table.

Table 14-3 Feature History for SNMP

Feature Name	Releases	Feature Information
SNMP Trap Control tab	4.2(1)	Added details of the new Control tab available from NX-OS Release 4.2(1).
SNMP Central Infra feature	4.2(1)	Added the new SNMP Central Infra feature details.
Configuring SNMP Users from the CLI	3.3(1a)	Removed des from the command switch(config)# snmp-server user user1 role1 auth md5 0xab0211gh priv 0x45abf342 localizedkey in To create or modify passwords for SNMP users from the CLI.