CHAPTER 26

SNMP Configuration

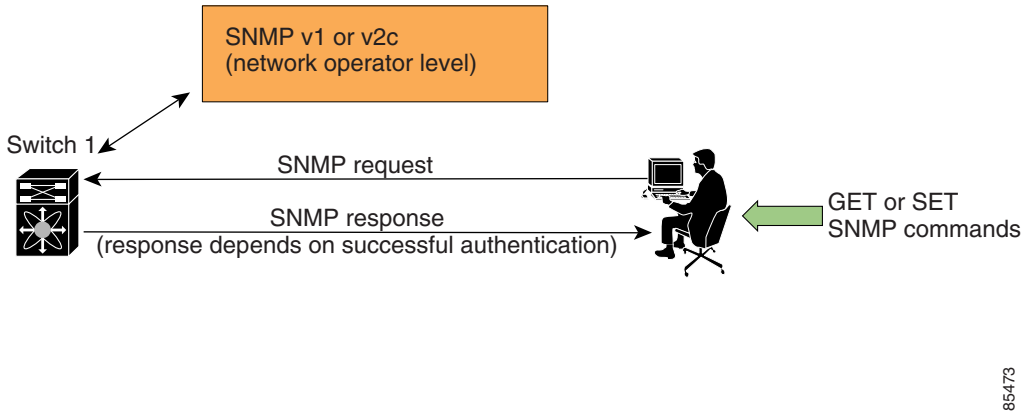
Fabric Manager provides the capability to configure SNMP for managing switches in the fabric.

This chapter includes the following sections:

About SNMP

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 26-1).

Figure 26-1 SNMP



SNMP Version 1 and Version 2c

SNMPv1 and 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

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. Uses DES or AES.

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.

Note Fabric Manager Release 2.1(2) or later supports forcing Fabric Manager or Device Manager to use SNMPv3 only. You must edit the batch or shell scripts in the bin directory where you installed Fabric Manager or Device Manager to uncomment the line that contains “snmp.voOnly”. When you open Fabric Manager or Device Manager, The Open dialog box shows only SNMPv3 login options.

SNMP v3 CLI User Management and AAA Integration

The Cisco MDS SAN-OS software implement 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.

As of Cisco MDS SAN-OS Release 2.0(1b), SNMP v3 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 AAA server. Once user authentication is verified, the SNMP PDUs are processed further. Additionally, the AAA server is also used to store user group names. SNMP uses the group names to apply the access/role policy that is locally available in the switch.

CLI and SNMP User Synchronization

In Cisco MDS SAN-OS Release 2.0(1b) or later, all updates to the CLI security database and the SNMP user database are synchronized. You can use the CLI password for accessing Fabric Manager or Device Manager and CLI. After you upgrade to Cisco MDS SAN-OS Release 2.0(1b) or later, you can continue using the SNMP password for Fabric Manager or Device Manager. If you use the CLI password for Fabric Manager or Device Manager login, you need to use the CLI password for future logins as well.

In Cisco MDS SAN-OS Release 2.0(1b) or later, users present in the prior release are assigned set of roles that is the union of both the CLI and the SNMP rules. Any configuration changes made to the user group, role, or password, results in the database synchronization for both SNMP and AAA.

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

Software Upgrade Synchronization

When you upgrade from an earlier release to Cisco MDS SAN-OS Release 2.0(1b) or later, the following synchronization steps occur:

- Existing SNMP users continue to retain the `auth` and `priv` information without any changes.
- If a user is not present in one database and is present in other database, the CLI user is created without any password (login is disabled) and the SNMP user is created with the noAuthNoPriv security level. Subsequently, the passwords and roles for these users will be synchronized.
- If the management station creates a SNMP user in the usmUserTable, this 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). See the "IP-ACL Configuration Guidelines" section on page 28-1.

Adding a Community String

To add a community string, follow these steps:

Step 1 From Fabric Manager, choose **Switches > Security->SNMP** from the Physical Attributes pane and click the **Communities** tab in the Information pane.

From Device Manager, choose **Security > SNMP** and click the **Communities** tab.

Step 2 Click **Create** in the Device Manager dialog box, or click the **Create Row** icon in Fabric Manager .

You see the Create Community string dialog box.

The dialog box in Fabric Manager also provides check boxes to specify one or more switches.

Step 3 Enter the community name in the Community field.

Step 4 Select the role from the check boxes in Device Manager or the drop-down list in Fabric Manager. In Fabric Manager, 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 (see the "Configuring Common Roles" section on page 25-2).

Step 5 Click **Create** to create the new entry or click **Close** to create the entry and close the dialog box.

Deleting a Community String

To delete a community string, follow these steps:

Step 1 From Fabric Manager, choose **Switches > Security->SNMP** from the Physical Attributes pane and click the **Communities** tab in the Information pane.

From Device Manager, choose **Security > SNMP** and click the **Communities** tab.

Step 2 Click the name of the community you want to delete.

Step 3 Click **Delete** in Device Manager or click the **Delete Row** icon in Fabric Manager.

Adding A Community String to the communities.properties File

If you have a mixed fabric of Cisco SAN-OS and Cisco FabricWare switches, we recommend that you securely open the fabric with a Cisco SAN-OS switch using SNMPv3. The SNMPv1/v2c community strings for the Cisco FabricWare switches should be entered in the communities.properties file.

To modify the communities.properties file using a text editor, follow these steps:

Step 1 On your workstation, go to the directory where you installed Fabric Manager. The default installation directory for Windows platforms is $HOME/cisco_mds9000/ and the default directory for UNIX platforms is /usr/local/cisco_mds9000/.

Step 2 Open the communities.properties file in a text editor.

Step 3 Add the SNMP community strings for your Cisco FabricWare switches as *ipaddress* = *read:write* , where:

- *ipaddress* is the IP address of the Cisco FabricWare switch.
- *read* is the SNMP read community string.
- *write* is the SNMP write community string.

The following example shows the addition of a pair of read:write community strings for switch 192.168.10.12:

```
192.168.10.12 = public:private
```

Step 4 Save the communities.properties file and restart Fabric Manager Server.

Understanding Users

Every Cisco MDS 9000 Family switch user has the account information stored by the system. Your authentication information, user name, user password, password expiration date, and role membership are stored in your user profile.

Adding a User

To add a user, follow these steps:

Step 1 From Fabric Manager, choose **Switches > Security->SNMP** from the Physical Attributes pane and click the **Communities** tab in the Information pane.

From Device Manager, choose **Security > SNMP** and click the **Users** tab.

Step 2 Click the **Create Row** icon in Fabric Manager or click **Create** in the Device Manager dialog box.

You see the Create Users dialog box.

The dialog box from Fabric Manager also provides check boxes to specify one or more switches.

Step 3 Enter the user name in the New User field.

Step 4 Select the role from the check boxes in Device Manager or the drop-down list in Fabric Manager. In Fabric Manager, 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 (see the "Configuring Common Roles" section on page 25-2).

Step 5 Enter the same authentication password for the user in the New Password and Confirm Password fields.

Step 6 Check the **Privacy** check box and complete the password fields to enable encryption of management traffic.

Enter the same new privacy password in the New Password and Confirm Password fields.

Step 7 Click **Create** to create the new entry or click **Close** close the dialog box without creating an entry.

Deleting a User

To delete a user, follow these steps:

Step 1 From Fabric Manager, choose **Switches > Security->SNMP** from the Physical Attributes pane and click the **Communities** tab in the Information pane.

From Device Manager, choose **Security > SNMP** and click the **Users** tab.

Step 2 Click the name of the user you want to delete.

Step 3 Click **Delete** in Device Manager or click the **Delete Row** icon in Fabric Manager.

Viewing SNMP Community and User Information

To view information about SNMP users, roles, and communities from Fabric Manager, choose **Security > SNMP** from the Physical tree and click the **Users, Roles,** or **Communities** tab. You see the list of SNMP users, roles, or communities in the Information pane.

To view this information from the Device Manager, choose **SNMP** from the Security menu. You see the SNMP dialog box.

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.

Assigning SNMPv3 Users to Multiple Roles

As of Cisco MDS SAN-OS Release 2.0(1b), the SNMP server user configuration is enhanced to accommodate multiple roles (groups) for SNMPv3 users. You map additional roles for the user at the time you create the user.

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

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

Step 1 Choose **Security > SNMP** and click the **Users** tab.

Step 2 Click **Create** in the Device Manager dialog box.You see the Create Communities dialog box.

Step 3 Enter the user name in the New User field.

Step 4 Select the multiple roles from the check boxes in Device Manager .

Step 5 Enter the same authentication password for the user in the New Password and Confirm Password fields.

Step 6 Check the **Privacy** check box and complete the password fields to enable encryption of management traffic.

Enter the same new privacy password in the New Password and Confirm Password fields.

Step 7 Click **Create** to create the new entry or click **Close** close the dialog box without creating an entry.

Configuring SNMP Notifications

You can configure the Cisco MDS switch to send notifications to SNMP managers when particular events occur. You can send these notifications as traps or inform requests. Traps are unreliable because the receiver does not send any acknowledgment when it receives a trap. The sender cannot determine if the trap was received. However, an SNMP manager that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives a response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

Note Use the SNMP-TARGET-MIB to obtain more information on trap destinations and inform requests. Refer to the *Cisco MDS 9000 Family MIB Quick Reference* for more information.

To configure SNMP notifications (traps or informs) using Fabric Manager, follow these steps:

Step 1 Choose **Switches > Events > SNMP Trap** 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 Destination Dialog box.

Step 4 Check the switches that you want to configure a new destination on.

Step 5 Set the destination IP address and UDP port.

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

Step 7 Optionally, set the inform timeout and retry values.

Step 8 Click **Create** to add this destination to the selected switches or click **Close** to discard any unsaved changes.

Step 9 Optionally, click the other tabs to enable specific notification types per switch.

Step 10 Click the **Apply changes** icon to create the entry or click **Undo Changes** to discard any unsaved changes.