Configuring Switch Security

The authentication, authorization, and accounting (AAA) strategy is used to verify identity of, grant access, and track the actions of remote users in all switches in the Cisco MDS 9000 Family. The Remote Access Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) provide AAA solutions.

Based on the user ID and password combination provided, switches perform local authentication using a local database or remote authentication using AAA server(s). A global, preshared, secret key authenticates communication between the AAA servers. This secret key can be configured for all AAA server groups or for only a specific AAA server. This kind of authentication provides a central configuration management capability.

This chapter contains the following topics:

Switch Management Security

Management security in any switch in the Cisco MDS 9000 Family is implemented using the Command-line interface (CLI) or Simple Network Management Protocol (SNMP).

SNMP Security

The SNMP agent supports security features for SNMPv1, SNMPv2c, and SNMPv3. Normal SNMP security mechanisms apply to all applications that use SNMP (for example, Cisco MDS 9000 Fabric Manager).

Users and roles configured through the CLI are different from users and roles configured through SNMP. These configurations do not directly correspond with each other. However, you can configure both CLI and SNMP identically, if required.

CLI Security

You can access the CLI using the Console (serial connection), Telnet, or Secure Shell (SSH). For each management path (console or Telnet and SSH), you can configure one or more of the following security control options: local, remote (RADIUS or TACACS+), or none.

- Remote security control
  - Using Remote Authentication Dial-In User Services (RADIUS).
  - Using Terminal Access Controller Access Control System plus (TACACS+).
- Local security control.
- Trivial authentication.

These authentication mechanisms can also be used to configure AAA for the following scenarios:

- iSCSI authentication
- Fibre Channel Security Protocol (FC-SP) authentication

Switch AAA Functionalities

Using CLI, you can configure Authentication, Authorization, and Accounting (AAA) switch functionalities on any switch in the Cisco MDS 9000 Family.

This section contains the following topics:

- Authentication, page 18-3
- Authorization, page 18-3
- Accounting, page 18-3
- Remote Authentication by AAA Servers, page 18-3
- Remote Authentication Guidelines, page 18-3
- Server Groups, page 18-4
- AAA Service Configuration Options, page 18-4

Authentication

Authentication is the process of verifying the identity of the person managing the switch. This identity verification is based on the user ID and password combination provided by the person trying to manage the switch. Cisco MDS 9000 Family switches allow you to perform local authentication (using the lookup database) or remote authentication (using one or more RADIUS or TACACS+ servers).

Authorization

By default, two roles exist in all switches:

- Network operator (network-operator)—Has permission to view the configuration only. The operator cannot make any configuration changes.
- Network administrator (network-admin)—Has permission to execute all commands and make configuration changes. The administrator can also create and customize up to 64 additional roles.

The two default roles cannot be changed or deleted. You can create additional roles and configure the following options:

- Assign user roles either locally or using remote AAA servers.
- Configure user profiles on a remote AAA server to contain role information. This role information is automatically downloaded and used when that user is authenticated through remote AAA server.

Accounting

Accounting refers to the log that is kept for each management session in a switch. This information may be used to generate reports for troubleshooting purposes and user accountability. Accounting can be implemented locally and remotely.

Remote Authentication by AAA Servers

AAA authentication provides the following advantages over local database authentication:

- Requires only one password to be shared between the switch and the AAA servers.
- Easier to manage user password lists for each switch in the fabric.
- AAA servers are deployed widely across enterprises and can be easily adopted.

Remote Authentication Guidelines

When you prefer using remote C servers, follow these guidelines:

- A minimum of one AAA server should be IP reachable.
- If all configured AAA servers are not reachable, the policy configured on the switch determines the authentication method.

- RADIUS servers are easily reachable if an overlay Ethernet LAN is attached to the switch. This is the recommended method.
- SAN networks connected to the switch should have at least one gateway switch connect to the Ethernet LAN containing the AAA servers. If you are using IP connectivity to reach an AAA server, the SAN connects to the switch.

Server Groups

You can specify remote AAA servers for authentication, authorization and accounting using server groups. A server group consists of remote AAA servers implementing the same AAA protocol. The purpose of a server group is to provide for fail-over servers in case a remote AAA server fails to response. If the first remote server in the group fails to respond, the next remote server in the group is tried until one of the servers sends a response. If all the AAA servers in the server group fails to respond, then that server group option is considered a failure. You can create a server group using the **aaa group server** command.

If required, you can specify multiple server groups. If the MDS switch encounters errors from the server(s) in the first group, it tries the servers in next server group.

AAA Service Configuration Options

AAA configuration in Cisco MDS switches is service based. You can have separate AAA configurations for following services:

- Telnet or SSH login—Choose **Switches** > **Security** > **SSH**.
- iSCSI authentication—Choose **End Devices** > **iSCSI** > **Global**.
- FC-SP authentication—Chose **Switches** > **Security** > **FC-SP**.

In general, server group, local, and none are the three options that can be specified for any service in an AAA configuration. Each option will be tried in the order specified. If all the methods fail, local is tried

Even if local is not specified as one of the options, it is tried when all other configured options fail.

Configuring RADIUS

Cisco MDS switches use the RADIUS protocol to communicate with remote AAA servers. You can configure multiple RADIUS servers and set timeout and retry counts.

This section defines the RADIUS operation, identifies its network environments, and describes its configuration possibilities.

This section contains the following topics:

- About RADIUS, page 18-5
- Configuring RADIUS Authentication, page 18-5
- Configuring RADIUS Servers, page 18-5
- Setting the RADIUS Server Address, page 18-5
- Setting the RADIUS Preshared Key, page 18-6

About RADIUS

RADIUS is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco MDS switches and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

RADIUS is a fully open protocol, distributed in source code format, that can be modified to work with any security system currently available on the market.

You can set the RADIUS server address, the RADIUS preshared key, the RADIUS server time-out interval, iterations of the RADIUS server, define vendor-specific attributes, and display RADIUS server details.

Configuring RADIUS Authentication

To configure RADIUS authentication from the Fabric Manager, choose **Security** > **Radius** from the menu tree.

To configure RADIUS authentication from the Device Manager, choose **Security** > **Radius (CLI)**.

Configuring RADIUS Servers

To configure RADIUS servers, perform the following steps:

Step 1 From the Device Manager, choose **Security** > **Radius** and click the **Servers** tab. You see the Radius dialog box with the Servers tab selected.

To configure RADIUS servers from the Fabric Manager, choose **Security** > **Radius** from the menu tree and click the **Servers** tab. You see the Radius information in the Information pane.

Step 2 To add a Radius server, click **Create** on the Device Manager dialog box, or click the **Create Row** icon on the Fabric Manager toolbar.

You see the Create Radius Server dialog box.(In Fabric Manager, you can specify the switches to which the configuration applies.)

Step 3 Complete the fields, and click **OK**.

Setting the RADIUS Server Address

You can add up to 64 RADIUS servers. RADIUS keys are always stored in encrypted form in persistent storage. The running configuration also displays encrypted keys. From Fabric Manager, choose **Switches** > **Security** > **Radius** > **Servers** to set RADIUS server addresses.

Setting the RADIUS Preshared Key

You need to configure the RADIUS preshared key to authenticate the switch to the RADIUS server. The length of the key is restricted to 65 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global key to be used for all RADIUS server configurations on the switch. From Fabric Manager, choose **Switches** > **Security** > **Radius** and click the **Defaults** tab to override this global key assignment.

Setting Iterations of the RADIUS Server

By default, a switch retries a RADIUS server connection only once. This number can be configured. The maximum is five retries per server. You can revert the retry number to its default. From Fabric Manager, choose **Switches** > **Security** > **Radius** > **Defaults**.

Defining Vendor-Specific Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific attributes (VSAs) between the network access server and the RADIUS server. The IETF uses attribute 26. VSAs allow vendors to support their own extended attributes that are not suitable for general use. The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. The Cisco vendor ID is 9, and the supported option is vendor type 1, which is named cisco-avpair. The value is a string with the following format:

```
protocol : attribute sep value *
```

where

- *protocol* is a Cisco attribute for a particular type of authorization
- *sep* is = for mandatory attributes and * is for optional attributes

When you use RADIUS servers to authenticate yourself to a Cisco MDS 9000 Family switch, the RADIUS protocol directs the RADIUS server to return user attributes, like authorization information, along with authentication results. This authorization information is specified through VSAs.

VSA Format

The following VSA protocol options are supported:

- Shell protocol—Used in Access-Accept packets to provide user profile information.
- Accounting protocol—Used in Accounting-Request packets. If a value contains any white spaces, it should be put within double quotation marks.

The following attributes are supported:

- roles— This attribute lists all the roles to which the user belongs. The value field is a string storing the list of group names delimited by white space. For example, if you belong to roles vsan-admin and storage-admin, the value field would be “vsan-admin storage-admin.” This subattribute is sent in the VSA portion of the Access-Accept frames from the RADIUS server, and it can only be used with the shell protocol value. This is an example using the roles attribute:

  ```
  Cisco-AVPair = shell:roles=”network-admin vsan-admin”
  ```

- accountinginfo—This attribute stores additional accounting information besides the attributes covered by a standard RADIUS accounting protocol. This attribute is only sent in the VSA portion of the Account-Request frames from the RADIUS client on the switch, and it can only be used with the accounting protocol value.

Configuring TACACS+

A Cisco MDS switch uses the Terminal Access Controller Access Control System plus (TACACS+) protocol to communicate with remote AAA servers. You can configure multiple TACACS+ servers and set timeout values.

This section contains the following topics:

About TACACS+

TACACS+ is a client-server protocol which uses TCP (TCP port 49) for transport requirements. All switches in the Cisco MDS 9000 Family provide centralized authentication using the TACACS+ protocol. The addition of TACACS+ support in SAN-OS 1.3(x) enables the following advantages over RADIUS authentication:

- Provides independent, modular AAA facilities--authorization can be done without authentication.
- Performs independent of servers if it is configured to its own database.
- TCP transport protocol to send data between the AAA client and server, using reliable transfers with a connection-oriented protocol
- Encrypts the entire protocol payload between the switch and the AAA server to ensure higher data confidentiality--the RADIUS protocol only encrypts passwords.

Advantages of TACACS+

This section provides a brief list of advantages that TACACS+ has over and RADIUS.

- Uses TCP protocol which has a connection-oriented transport
- Provides built-in transport support
- Provides a separate acknowledgment that a request has been received
- Provides immediate indication of a crashed, or not running, server
- Detects server crashes out-of-band with actual requests

- Maintains simultaneous connections to multiple servers
- Adapts to growing, as well as congested networks

Enabling TACACS+

By default, the TACACS+ feature is disabled in all switches in the Cisco MDS 9000 Family. You must explicitly enable the TACACS+ feature to access the configuration and verification commands for fabric authentication. When you disable this feature, all related configurations are automatically discarded.

Setting the TACACS+ Server Address

If a secret key is not configured for a configured server, a warning message is issued and the global secret encryption key is automatically used.

Setting the Secret Key

From Fabric Manager, choose **Switches** > **Security** > **TACACS+** > **Defaults** to configure global values for the key for all TACACS+ servers.

Secret keys configured for individual servers override the globally configured values.

Setting the Timeout Value

From Fabric Manager, choose **Switches** > **Security** > **TACACS+** > **Defaults** to configure global timeout values for all TACACS+ servers.

Timeout values configured for individual servers override the globally configured values.

Defining Custom Attributes for Roles

MDS uses TACACS+ custom attribute for service shell to configure the roles to which a user belongs. TACACS+ attributes are specified as name=value format. The attribute name for this custom attribute is cisco-av-pair. The following example illustrates how to specify roles using this attribute:

```
cisco-av-pair=shell:roles=”network-admin vsan-admin”
```

TACACS+ custom attributes can be defined on an ACS server for various services (for example, shell). MDS requires the TACACS+ custom attribute for service shell to be used for defining roles.

Configuring Server Groups

You can specify one or more remote AAA servers to authenticate users using server groups. All members of a group must belong to the same protocol: either RADIUS or TACACS+. The servers are tried in the same order in which you configure them.

You can configure these server groups at any time but they only take effect when you apply them to a AAA service. From Fabric Manager, choose **Switches > Security > AAA > Server Groups**.

You can specify one or more remote AAA servers to authenticate users using server groups.

Local AAA

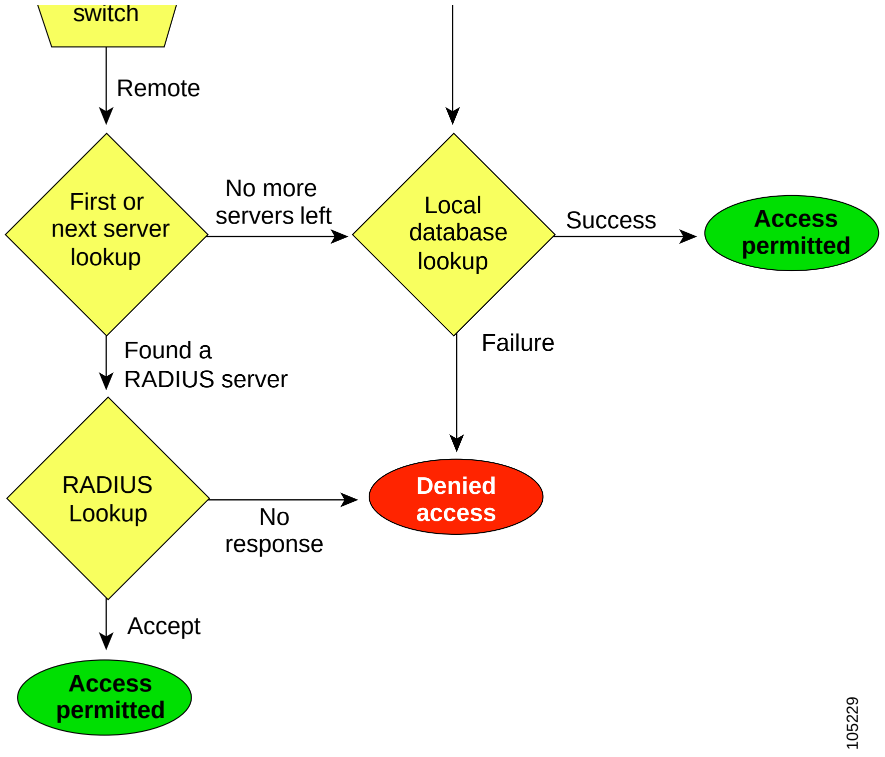
The system maintains the user name and password locally and stores the password information in encrypted form. You are authenticated based on the locally stored user information.

Authentication and Authorization Process

Authentication is the process of verifying the identity of the person managing the switch. This identity verification is based on the user ID and password combination provided by the person trying to manage the switch. The Cisco MDS 9000 Family switches allow you to perform local authentication (using the lookup database) or remote authentication (using one or more RADIUS servers or TACACS+ servers).

The following steps explain the authorization and authentication process. shows a flow chart of the process.

Figure 18-1 Switch Authorization and Authentication Flow



Step 1 When you can log in to the required switch in the Cisco MDS 9000 Family, you have the option to use the Telnet, SSH, or Console login options.

Step 2 When you configure server groups using the server group authentication method, an authentication request is sent to the first AAA server in the group.

- If the AAA server fails to respond, then the next AAA server will be tried and so on until the remote server responds to the authentication request.
- If all AAA servers in the server group fail to respond, then the servers in the next server group are tried.
- If all configured methods fails, then local database is used for authentication.

Step 3 When you are successfully authenticated through a remote AAA server, then the following possibilities apply:

- If AAA server protocol is RADIUS, the user roles specified in cisco-av-pair attribute is downloaded with authentication response
- If AAA server protocol is TACACS+, then another request is sent to the same server to get the user roles specified as custom attributes for shell
- If user roles were not retrieved successfully from remote AAA server, then the user will have role of network-operator assigned once he logs in.

Step 4 If your user name and password are successfully authenticated, you are allowed to log in.

Configuring Role-Based CLI Authorization

Switches in the Cisco MDS 9000 Family perform authentication based on roles. Role-based authorization limits access to switch operations by assigning users to roles. This kind of authentication restricts you to management operations based on the roles to which you have been added.

When you execute a command, perform command completion, or obtain context sensitive help, the switch software allows the operation to progress if you have permission to access that command.

Each role can contain multiple users and each user can be part of multiple roles. For example, if role1 users are only allowed to perform configuration commands, and role2 users are only allowed to perform debug commands, then if Joe belongs to both role1 and role2, he can perform configuration as well as debug commands.

If you belong to multiple roles, you can execute a superset of all the commands permitted by these roles. Access to a command takes priority over being denied access to a command. For example, suppose you belong to a TechDocs group and you were denied access to configuration commands. However, you also belong to the engineering group and have access to configuration commands. In this case, you will have access to configuration commands.

Tip Any role, when created, does not allow access to the required commands immediately. The administrator must configure appropriate rules for each role to allow access to the required commands.

Configuring Rules and Features for Each Role

A rule specifies operations that can be performed by a specific role. Each rule consists of a command type (for example, **config**, **clear**, **show**, **exec**, **debug**), and an optional feature name (for example, FSPF, zone, VSAN, fcping, interface).

Configuring the VSAN Policy

Configuring the VSAN policy requires the ENTERPRISE_PKG license.

You can configure a role so that it only allows commands to be performed for a selected set of VSANs. By default, the VSAN policy for any role is **permit**. In other words, the role can perform commands configured by the rule in all VSANs. In order to selectively allow VSANs for a role, the VSAN policy needs to be set to **deny** and then the appropriate VSANs need to be permitted.

Users configured in roles where the VSAN policy set to **deny** cannot modify configuration for E ports. They can only modify configuration for F or FL ports (depending on whether the configured rules allow such configuration to be made). This is to prevent such users from modifying configurations that may impact the core topology of the fabric.

Tip Roles can be used to create VSAN administrators. Depending on the configured rules, these VSAN administrators can configure MDS features (for example, zone, fcdomain, VSAN properties) for their VSANs without affecting other VSANs. Also, if the role permits operations in multiple VSANs, then the VSAN administrators can change VSAN membership of F or FL ports among these VSANs.

Users belonging to roles in which the VSAN policy is set to **deny** are referred to as VSAN-restricted users. These users cannot perform the following functions that require the startup configuration to be viewed or modified:

- **copy running startup**
- **show startup**
- **show running-config diff**
- **copy startup** <destination>
- **copy** <source> **startup** commands.

For information on these commands, refer to the *Cisco MDS 9000 Family Command Reference*.

Recovering Administrator Password

An administrator can recover a password from a local console connection.

The password recovery procedure must be performed on the supervisor module that becomes the active supervisor module after the recovery procedure is completed. To ensure the other supervisor module does not become the active module, you have two options:

Password recovery is not possible from a Telnet or SSH session.

To recover a administrator password, refer to the *Cisco MDS 9000 Family Command Reference*.

Configuring SSH Services

The Telnet service is enabled by default on all Cisco MDS 9000 Family switches. Before enabling the SSH service, generate a host key pair.

Enabling SSH Service

By default, the SSH service is disabled.

Generating an SSH Host Key Pair

Be sure to have an SSH host key pair with the appropriate version before enabling the SSH service. The SSH service accepts three types of key pairs for use by SSH versions 1 and 2. Generate the SSH host key pair according to the SSH client version used. The number of bits specified for each key pair ranges from 768 to 2048.

- The **rsa1** option generates the RSA1 key pair for the SSH version 1 protocol.
- The **dsa** option generates the DSA key pair for the SSH version 2 protocol.
- The **rsa** option generates the RSA key pair for the SSH version 2 protocol.

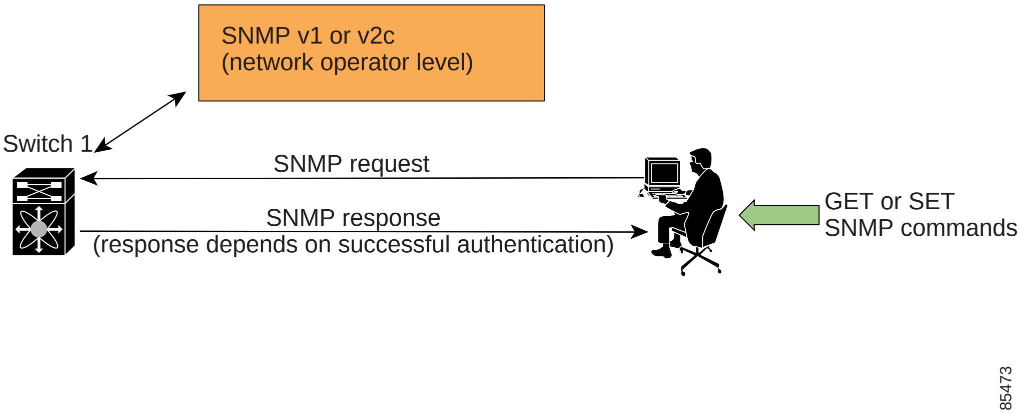
Using the force Option

If the SSH key pair option is already generated for the required version, use the **force** option to overwrite the previously generated key pair.

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 18-2.)

Figure 18-2 SNMP Security



Users and roles configured through the CLI are different from users and roles configured through SNMP. These configurations do not directly correspond with each other. However, you can configure both CLI and SNMP identically, if required. See the "Creating Common Roles" section on page 18-18 for additional information.

SNMP users are different from CLI users. SNMP users also have role-based authentication for roles and authorization purposes.

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.

Adding a Community String

To add a community string, follows these steps:

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

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

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

The Create Community string dialog box displays. (The dialog box from Fabric Manager also provides check boxes to specify one or more switches.)

Step 3 Enter the community name in the Community field.

Step 4 Choose the role from the drop-down list. In Fabric Manager, you can enter a new role name in the field if you do not want to choose one from the list. If you enter a new role name, you must go back and configure this role appropriately (see the "Configuring Common Roles" section on page 18-16).

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, follows these steps:

Step 1 From Fabric Manager, select **Security** > **SNMP** from the Physical pane menu and click the **Communities** tab in the Information pane.

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

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

Step 3 Click **Delete** (Device Manager) or the **Delete Row** icon (Fabric Manager).

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.

Adding SNMP Users

To add SNMP users, follows these steps:

Step 1 From Fabric Manager, select **Security** > **SNMP** from the Physical pane menu and click the **Users** tab in the Information pane.

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

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

The Create Users dialog box displays. (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 drop-down list. In Fabric Manager, you can enter a new role name in the field if you do not want to select one from the list. If you enter a new role name, you must go back and configure this role appropriately (see the "Configuring Common Roles" section on page 18-16).

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

Step 6 To enable encryption of management traffic, click the **Privacy** check box and complete the password fields.

Enter the authentication password in the Clone Password field to use the same password. Enter a new password twice in the New Password and Confirm Password fields.

Step 7 Click **Create** to create the new entry, or click **Close** to create the entry and close the dialog box.

Deleting SNMP Users

To delete SNMP users, follows these steps:

Step 1 From Fabric Manager, select **Security** > **SNMP** from the Physical pane menu and click the **Users** tab in the Information pane.

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

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

Step 3 Click **Delete** (Device Manager) or the **Delete Row** icon (Fabric Manager).

Configuring and Creating SNMP User Roles

To configure users roles, choose **Security** > **SNMP** from Device Manager, and click the **Roles** tab.

To create a new role, follow these steps:

Step 1 Click **Create**. You see the Create Roles dialog box.

Step 2 Enter an identifier for the role in the Role field.

Step 3 Select one of the following security levels:

- authNoPrv—Authentication without encryption
- AuthPriv—Authentication with encryption

Step 4 For Read access, click the **All** radio button to enable full read access or click **List** and check each check box in the list to enable read access to specific information.

Step 5 For Write access, click the **All** radio button to enable full read access or click **List** and check each check box in the list to enable read access to specific information.

Step 6 Click **Apply** to create the new role, or click **OK** to create the role and close the window.

Viewing SNMP Community and User Information

To view information about SNMP users, roles, and communities from Fabric Manager, choose **Security > SNMP** from the Physical pane menu 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 **Security > SNMP**. The SNMP dialog box displays.

Group-Based SNMP Access

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.

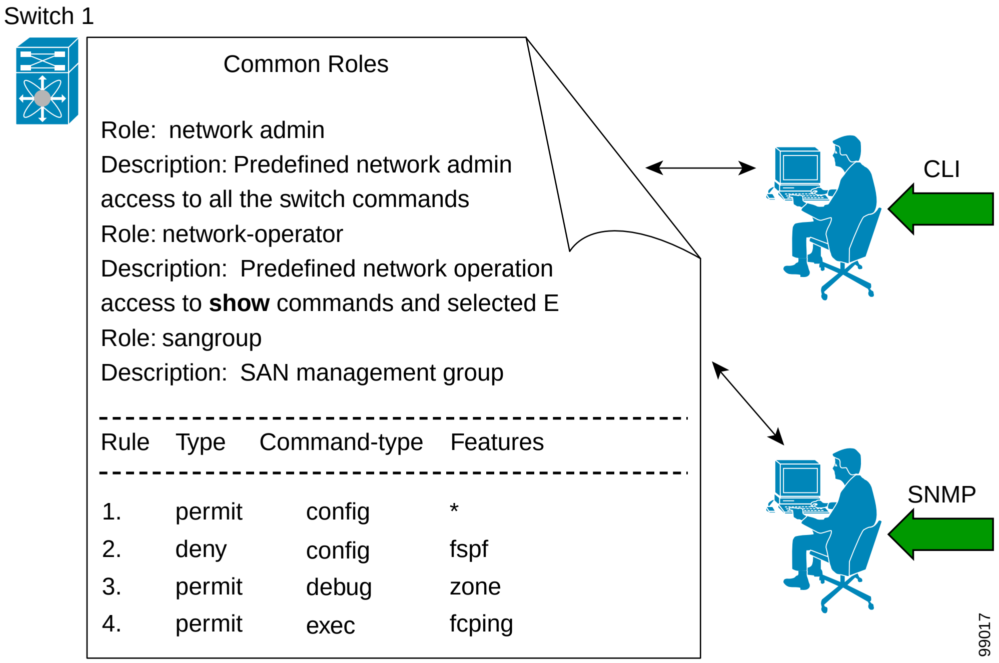
You can begin communicating with the agent once the your user name is created, your roles are set up by your administrator, and you are added to the roles.

Users configured through the CLI are different from users configured through SNMP. These configurations do not directly correspond with each other. However, you can configure both CLI and SNMP identically, if required.

Configuring Common Roles

From Release 1.2(x), CLI and SNMP in all switches in the Cisco MDS 9000 Family use common roles. You can use SNMP to modify a role that was created using CLI and vice versa.

Figure 18-3 Common Roles



Common Roles

Role: network admin
Description: Predefined network admin
access to all the switch commands
Role: network-operator
Description: Predefined network operation
access to **show** commands and selected E
Role: sangroup
Description: SAN management group

Rule	Type	Command-type	Features
1.	permit	config	*
2.	deny	config	fspf
3.	permit	debug	zone
4.	permit	exec	fcping

Each role in SNMP is the same as a role created or modified through the CLI. Common Roles allow you to use a set of rules to set the scope of VSAN security. Each role can be restricted to one or more VSANs as required.

You can create new roles or modify existing roles using SNMP or the CLI.

To configure Common Roles from the Device Manager, choose **Common Roles** from the Security menu. You can then access the Rules dialog box to configure the set of rules. To configure Common Roles from Fabric Manager, choose **Security** > **SNMP** and click the **Roles** tab in the Information pane. Fabric Manager uses a default rules set for roles; therefore, no Rules dialog box is displayed.

See the "Creating Common Roles" section on page 18-18 for additional information.

Creating and Modifying Users

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

- SNMP—Create a user as a clone of an existing user in the vsmUserTable on the switch. Once you have created the user, change the cloned secret key before activating the user. Refer to RFC2574.

  You must explicitly configure password(s) for SNMP users. The SNMP user passwords are not generated as the part of the configuration file as they are not portable across devices. The password is limited to a minimum of 8 characters and a maximum of 64 characters.

  An SNMP user must be created on each switch to which the user requires access. If the user is managing 10 switches, each of the 10 switches must have the SNMP user defined.

- CLI—You can create a user or modify an existing user using the **snmp-server user** command.

By default, only two roles are available in a Cisco MDS 9000 Family switch—network-operator and network-admin. You can also use any role that is configured in the Common Roles database.

Creating Common Roles

To create a common role in Fabric Manager, perform the following steps:

Step 1 Choose **Security > SNMP** from the Physical pane menu tree, and click the **Roles** tab in the Information pane.

Step 2 Click the **Create Row** icon in the toolbar.

The Roles -> Create dialog box displays.

Step 3 Choose the switches for which you want to configure the role.

Step 4 Enter the name of the role in the Name field.

Step 5 Enter the description of the role in the Description field.

Step 6 Check (or uncheck) the **Has Config and Exec Permission** check box.

If you check the check box, your role will have read, write, and create permission. If you do not check the check box, your role will have read-only permission.

Step 7 Click **Enable** to enable the VSAN scope.

Step 8 Enter the scope in the Scope field.

Step 9 Click **Create** to create the Role, or click **Close** to close the Role dialog without creating the common role.

To create a common role in Device Manager, perform the following steps:

Step 1 Choose **Security > Common Roles**. The Common Roles dialog box displays.

Step 2 Click **Create**.

The Create Common Roles dialog box displays.

Step 3 Enter the name of the common role in the Name field.

Step 4 Enter the description of the common role in the Description field.

Step 5 Click **Enable** to enable the VSAN scope.

Step 6 Enter the scope in the Scope field.

Step 7 Click **Rules** to view the rules for the role, and select the rules you want to enable. Then click **Close** to close the Rules dialog.

The Rules dialog may take a few minutes to display.

Step 8 Click **Create** to create the common role, or click **Close** to close the Common Role dialog without creating the common role.

Editing Common Role Rules (Device Manager Only)

To edit the rules for a common role, perform the following steps:

Step 1 From the Device Manager, choose **Security > Common Roles**.

The Common Roles dialog box displays.

Step 2 Click once on the common role for which you want to edit the rules.

Step 3 Click **Rules** to view the rules for the role.

The Rules dialog may take a few minutes to display.

Step 4 Edit the rules you want to enable or disable for the common role.

Step 5 Click **Apply** to apply the new rules and close the Rules dialog, or click **Close** to close the Rules dialog without applying the rules.

Step 6 Click **Apply** to create the common role, or click **Close** to close the Common Role dialog without creating the common role.

Deleting Common Roles

To delete a common role, perform the following steps:

Step 1 From the Device Manager, choose **Security > Common Roles**. The Common Roles dialog box displays.

From Fabric Manager, choose **Security > SNMP** from the Physical pane menu tree, and click the **Roles** tab in the Information pane.

Step 2 Click once to select the common role you want to delete.

Step 3 Click **Delete** to delete the common role.

Assigning Users to Roles

Once the user and the role are created, the administrator should configure an entry in the vacmSecurityToGroupTable to add the configured user to a configured role.

- To assign users to roles through SNMP, refer to RFC2575.
- To assign users to roles through the CLI, refer to the procedure specified in the *Cisco MDS 9000 Family Command Reference*.

Default Security Settings

Table 18-1 lists the default settings for all security features in any switch.

Table 18-1 Default Security Settings

Parameters	Default
Roles in each switch (for CLI and SNMP users)	Two default roles—network-operator and network-admin.
AAA authentication login	Local authentication is enabled. If the Telnet or SSH options are not specified, the command applies to both.
Telnet server	Enabled.
Accounting log file size on local disk	15,000 bytes.
User’s account expiration	Does not expire unless you explicitly configure it to expire.
User name	admin.
User password	admin.
Configured RADIUS sever	Allows access to all RADIUS severs.
RADIUS server timeout interval	The default time-out is one (1) seconds.
RADIUS preshared key	No key is configured.
RADIUS key encryption	clear text (0)—Not encrypted.
RADIUS server connection attempts	A switch tries to connect to a RADIUS server once (1).
RADIUS Authentication port	UDP port 1812.
RADIUS Accounting port	UDP port 1813.
Server key encryption	clear text (0)—Not encrypted.
TACACS+	Disabled
Configured TACACS+ sever	Allows access to all TACACS+ severs.
TACACS+ server timeout interval	The default time-out is one (5) seconds.
TACACS+ preshared key	No key is configured.
TACACS+ key encryption	clear text (0)—Not encrypted
TACACS+ server connection attempts	A switch tries to connect to a TACACS+ server once (1).
TACACS+ Authentication port	UDP port 49.
VSAN policy	Permit.

Restricting Switch Access

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