CHAPTER 41

Configuring RADIUS and TACACS+

The authentication, authorization, and accounting (AAA) feature verifies the identity of, grants access to, and tracks the actions of users managing a switch. All Cisco MDS 9000 Family switches use RADIUS and TACACS+ protocols to provide solutions using remote AAA servers.

Based on the user ID and password combination provided, switches perform local authentication or authorization using the local database or remote authentication or authorization using a AAA server. A preshared secret key provides security for communication between the switch and AAA servers. This secret key can be configured for all AAA servers or for only a specific AAA server. This security feature provides a central management capability for AAA servers.

This chapter includes the following sections:

Switch Management Security

Management security in any switch in the Cisco MDS 9000 Family provides security to all management access methods, including the command-line interface (CLI) or Simple Network Management Protocol (SNMP).

This section includes the following topics:

Fabric Manager Security Options

You can access Fabric Manager using the console (serial connection), Telnet, or Secure Shell (SSH). For each management path (console, 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 RADIUS. See the "Configuring RADIUS Server Monitoring Parameters" section on page 41-7.
  - Using TACACS+. See the "Configuring TACACS+ Server Monitoring Parameters" section on page 41-14.
- Local security control. See the "Local AAA Services" section on page 41-26.

These security features can also be configured for the following scenarios:

- iSCSI authentication (see the "iSCSI Authentication Setup Guidelines and Scenarios" section on page 50-56).
- Fibre Channel Security Protocol (FC-SP) authentication (see Chapter 45, "Configuring FC-SP and DHCHAP")

SNMP Security Options

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

SNMP security options also apply to the Fabric Manager and Device Manager.

See Chapter 40, "Configuring SNMP".

Switch AAA

Using the CLI or Fabric Manager, you can configure AAA switch functionalities on any switch in the Cisco MDS 9000 Family.

This section includes the following topics:

- Authentication, page 41-3
- Authorization, page 41-3
- Accounting, page 41-3
- Remote AAA Services, page 41-4
- Remote Authentication Guidelines, page 41-4
- Server Groups, page 41-4
- AAA Configuration Options, page 41-4
- Authentication and Authorization Process, page 41-6

Authentication

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

Note When you log in to a Cisco MDS switch successfully using the Fabric Manager or Device Manager through Telnet or SSH and if that switch is configured for AAA server-based authentication, a temporary SNMP user entry is automatically created with an expiry time of one day. The switch authenticates the SNMPv3 protocol data units (PDUs) with your Telnet or SSH login name as the SNMPv3 user. The management station can temporarily use the Telnet or SSH login name as the SNMPv3 **auth** and **priv** passphrase. This temporary SNMP login is only allowed if you have one or more active MDS shell sessions. If you do not have an active session at any given time, your login is deleted and you will not be allowed to perform SNMPv3 operations.

Note Fabric Manager does not support AAA passwords with trailing white space, for example “passwordA“.

Authorization

The following authorization roles exist in all Cisco MDS 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.
- Default-role—Has permission to use the GUI (Fabric Manager and Device Manager). This access is automatically granted to all users for accessing the GUI.

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

- Configure role-based authorization by assigning user roles 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 the user is authenticated through the remote AAA server.

Note If a user belongs only to one of the newly created roles and that role is subsequently deleted, then the user immediately defaults to the network-operator role.

Accounting

The accounting feature tracks and maintains a log of every management configuration used to access the switch. This information can be used to generate reports for troubleshooting and auditing purposes. Accounting logs can be stored locally or sent to remote AAA servers.

Remote AAA Services

Remote AAA services provided through RADIUS and TACACS+ protocols have the following advantages over local AAA services:

- User password lists for each switch in the fabric can be managed more easily.
- AAA servers are already deployed widely across enterprises and can be easily adopted.
- The accounting log for all switches in the fabric can be centrally managed.
- User role mapping for each switch in the fabric can be managed more easily.

Remote Authentication Guidelines

If you prefer using remote AAA servers, follow these guidelines:

- A minimum of one AAA server should be IP reachable.
- Be sure to configure a desired local AAA policy as this policy is used if all AAA servers are not reachable.
- AAA servers are easily reachable if an overlay Ethernet LAN is attached to the switch (see Chapter 52, “Configuring IP Storage”). We recommend this method.
- SAN networks connected to the switch should have at least one gateway switch connected to the Ethernet LAN reaching the AAA servers.

Server Groups

You can specify remote AAA servers for authentication, authorization, and accounting using server groups. A server group is a set of remote AAA servers implementing the same AAA protocol. The purpose of a server group is to provide for failover servers in case a remote AAA server fails to respond. 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 fail to respond, then that server group option is considered a failure. If required, you can specify multiple server groups. If the Cisco MDS switch encounters errors from the servers in the first group, it tries the servers in the next server group.

AAA Configuration Options

AAA configuration in Cisco MDS 9000 Family switches is service based. You can have separate AAA configurations for the following services:

- Telnet or SSH login (Fabric Manager and Device Manager login)
- Console login
- iSCSI authentication (see Chapter 50, “Configuring iSCSI”)
- FC-SP authentication (see Chapter 45, “Configuring FC-SP and DHCHAP”)
- Accounting

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

Caution Cisco MDS SAN-OS does not support all numeric usernames, whether created with TACACS+ or RADIUS, or created locally. Local username with all numerics cannot be created. If an all numeric username exists on an AAA server and is entered during login, the user is not logged in.

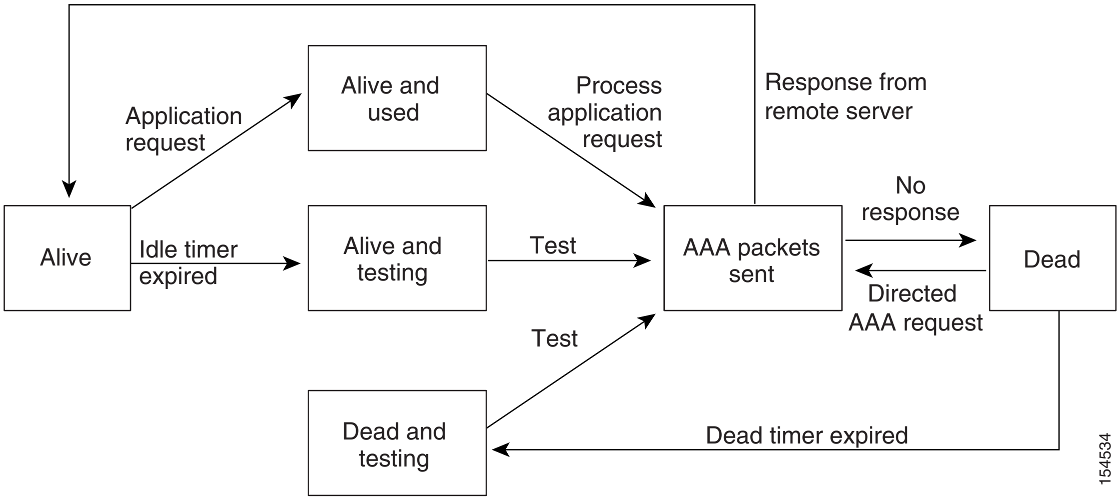
Note Even if local is not specified as one of the options, it is tried when all other configured options fail.

When RADIUS times out, local login is always attempted. For this local login to be successful, a local account for the user with the same password should exist, and the RADIUS timeout and retries should take less than 40 seconds. The user is authenticated if the username and password exist in the local authentication configuration.

AAA Server Monitoring

An unresponsive AAA server introduces a delay in the processing of AAA requests. An MDS switch can periodically monitor an AAA server to check whether it is responding (or alive) to save time in processing AAA requests. The MDS switch marks unresponsive AAA servers as dead and does not send AAA requests to any dead AAA servers. An MDS switch periodically monitors dead AAA servers and brings them to the alive state once they are responding. This monitoring process verifies that an AAA server is in a working state before real AAA requests are sent its way. Whenever an AAA server changes to the dead or alive state, an SNMP trap is generated and the MDS switch warns the administrator that a failure is taking place before it can impact performance. See Figure 41-1 for AAA server states.

Figure 41-1 AAA Server States



Note The monitoring interval for alive servers and dead servers is different and can be configured by the user. The AAA server monitoring is performed by sending a test authentication request to the AAA server.

The user name and password to be used in the test packet can be configured.

See the "Configuring RADIUS Server Monitoring Parameters" section on page 41-7.

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 managing 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:

Step 1 You can log in to the required switch in the Cisco MDS 9000 Family, using the Telnet, SSH, Fabric Manager/Device Manager, or console login options.

Step 2 When you have configured 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 is contacted 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 contacted.
- If all configured methods fail, then the local database is used for authentication.

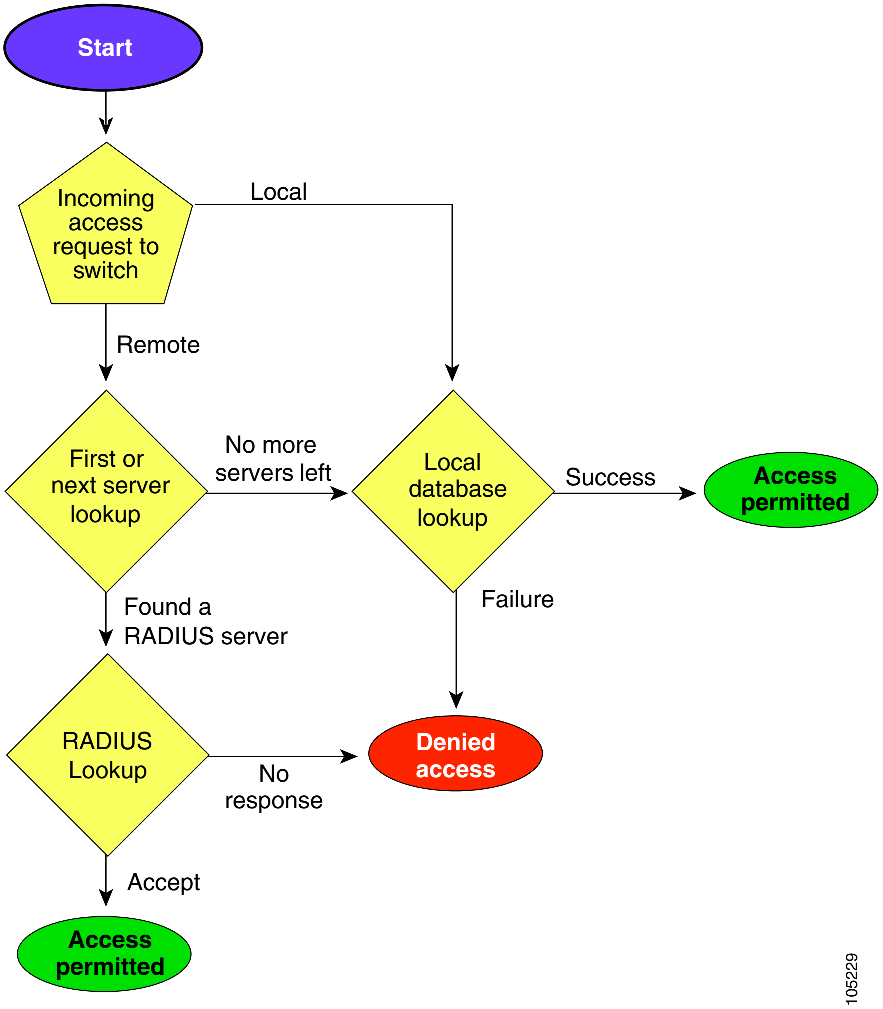
Step 3 When you are successfully authenticated through a remote AAA server, then the following possible actions are taken:

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

Step 4 When your user name and password are successfully authenticated locally, you are allowed to log in, and you are assigned the roles configured in the local database.

Figure 41-2 shows a flow chart of the authorization and authentication process.

Figure 41-2 Switch Authorization and Authentication Flow



Note No more server groups left = no response from any server in all server groups.
No more servers left = no response from any server within this server group.

Configuring RADIUS Server Monitoring Parameters

Cisco MDS 9000 Family switches can use the RADIUS protocol to communicate with remote AAA servers. You can configure multiple RADIUS servers and server groups and set timeout and retry counts.

RADIUS is a distributed client/server protocol that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco MDS 9000 Family switches and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

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

This section includes the following topics:

About RADIUS Server Default Configuration

Fabric Manager allows you to set up a default configuration that can be used for any RADIUS server that you configure the switch to communicate with. The default configuration includes:

- Encryption type
- Timeout value
- Number of retransmission attempts
- Allowing the user to specify a RADIUS server at login

About the Default RADIUS Server Encryption Type and 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 64 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.

You can override this global key assignment by explicitly using the **key** option when configuring an individual RADIUS server.

Configuring the Default RADIUS Server Encryption Type and Preshared Key

To configure the default RADIUS server encryption type and preshared key using Fabric Manager, follow these steps:

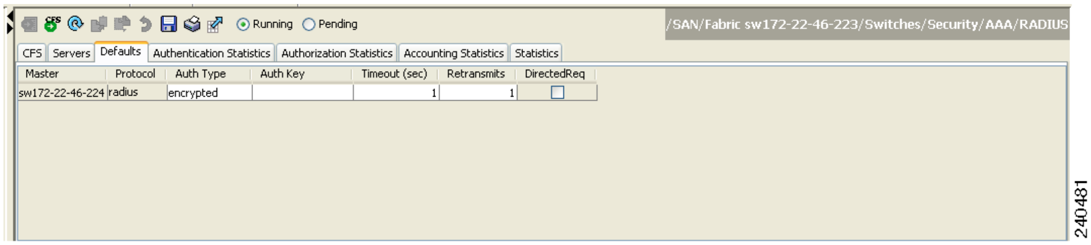
Step 1 Expand **Switches > Security > AAA**, and then select **RADIUS.**

You see the RADIUS configuration in the Information pane.

Step 2 Click the **Defaults** tab.

You see the RADIUS default settings as shown in Figure 41-3.

Figure 41-3 RADIUS Default Settings



Master	Protocol	Auth Type	Auth Key	Timeout (sec)	Retransmits	DirectedReq
sw172-22-46-224	radius	encrypted		1	1	□

Step 3 Select **plain** or **encrypted** from the AuthType drop-down menu.

Step 4 Set the key in the Auth Key field.

Step 5 Click the **Apply Changes** icon to save the changes.

Setting the Default RADIUS Server Timeout Interval and Retransmits

By default, a switch retries transmission to a RADIUS server only once before reverting to local authentication. You can increase this number up to a maximum of five retries per server. You can also configure the timeout value for the RADIUS server.

To configure the number of retransmissions and the time between retransmissions to the RADIUS servers using Fabric Manager, follow these steps:

Step 1 Expand **Switches > Security > AAA a**nd then select **RADIUS.**

You see the RADIUS configuration in the Information pane.

Step 2 Choose the **Defaults** tab.

You see the RADIUS default settings.

Step 3 Fill in the Timeout and Retransmits fields for authentication attempts.

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

About RADIUS Servers

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. When you configure a new RADIUS server, you can use the default configuration or modify any of the parameters to override the default RADIUS configuration.

Configuring a RADIUS Server

To configure a RADIUS server and all its options using Fabric Manager, follow these steps:

Step 1 Expand **Switches > Security > AAA,** and then select **RADIUS**.

You see the RADIUS configuration in the Information pane.

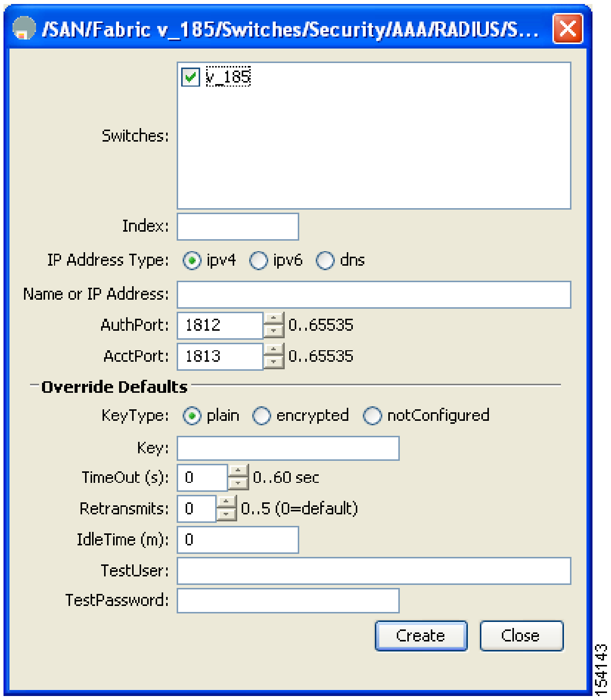
Step 2 Click the **Servers** tab.

You see any existing RADIUS servers.

Step 3 Click **Create Row** to add a new RADIUS server.

You see the Create RADIUS Server dialog box shown in Figure 41-4.

Figure 41-4 Create RADIUS Server



/SAN/Fabric v_185/Switches/Security/AAA/RADIUS/S...

Switches: ☑ v_185

Index:

IP Address Type: ● ipv4 ○ ipv6 ○ dns

Name or IP Address:

AuthPort: 1812 0..65535

AcctPort: 1813 0..65535

Override Defaults

KeyType: ● plain ○ encrypted ○ notConfigured

Key:

TimeOut (s): 0 0..60 sec

Retransmits: 0 0..5 (0=default)

IdleTime (m): 0

TestUser:

TestPassword:

Step 4 Select the switches that you want to assign as RADIUS servers.

Step 5 Assign an index number to identify the RADIUS server.

Step 6 Select the IP address type for the RADIUS server.

Step 7 Fill in the IP address or name for the RADIUS server.

Step 8 Optionally, modify the authentication and accounting ports used by this RADIUS server.

Step 9 Select the appropriate key type for the RADIUS server.

Step 10 Select the TimeOut value in seconds. The valid range is 0 to 60 seconds.

Step 11 Select the number of times the switch tries to connect to a RADIUS server(s) before reverting to local authentication.

Step 12 Enter the test idle time interval value in minutes. The valid range is 1 to 1440 minutes.

Step 13 Enter the test user with the default password. The default username is test.

Step 14 Click **Create** to save these changes.

Configuring the Test Idle Timer

The test idle timer specifies the interval during which a RADIUS server receives no requests before the MDS switch sends out a test packet.

Note The default idle timer value is 0 minutes. When the idle time interval is 0 minutes, periodic RADIUS server monitoring is not performed.

To configure the test idle timer, see "Configuring a RADIUS Server" section on page 41-10.

Configuring Test User Name

You can configure a username and password for periodic RADIUS server status testing. You do not need to configure the test username and password to issue test messages to monitor RADIUS servers. You can use the default test username (test) and default password (test).

Note We recommend that the test username not be the same as an existing username in the RADIUS database for security reasons.

To configure the optional username and password for periodic RADIUS server status testing, see "Configuring a RADIUS Server" section on page 41-10.

About Validating a RADIUS Server

As of Cisco SAN-OS Release 3.0(1), you can periodically validate a RADIUS server. The switch sends a test authentication to the server using the username and password that you configure. If the server does not respond to the test authentication, then the server is considered non responding.

Note For security reasons we recommend that you do not use a username that is configured on your RADIUS server as a test username.

You can configure this option to test the server periodically, or you can run a one-time only test.

Periodically Validating a RADIUS Server

To configure the switch to periodically test a RADIUS server using Fabric Manager, follow these steps:

Step 1 Expand **Switches > Security > AAA**, and then select **RADIUS**.

You see the RADIUS configuration in the Information pane.

Step 2 Click the **Servers** tab.

You see any existing RADIUS servers.

Step 3 Click **Create Row** to add a new RADIUS server.

You see the Create RADIUS Server dialog box (see Figure 41-4).

Step 4 Fill in the IP address.

Step 5 Modify the authentication and accounting ports used by this RADIUS server.

Step 6 Fill in the TestUser field and, optionally, the TestPassword field. The default password for the test is **Cisco**.

Step 7 Set the IdleTime field for the time that the server is idle before you send a test authentication.

Step 8 Click **Create** to save these changes.

Displaying RADIUS Server Statistics

To display RADIUS server statistics using Fabric Manager, follow these steps:

Step 1 Expand **Switches > Security > AAA,** and then select **RADIUS**.

You see the RADIUS configuration in the Information pane.

Step 2 Click the **Statistics** tab.

You see the RADIUS server statistics.

About Users Specifying a RADIUS Server at Login

By default, an MDS switch forwards an authentication request to the first server in the RADIUS server group. You can configure the switch to allow the user to specify which RADIUS server to send the authenticate request by enabling the directed request option. If you enable this option, the user can log in as *username@hostname*, where the *hostname* is the name of a configured RADIUS server.

Allowing Users to Specify a RADIUS Server at Login

To allow users logging into an MDS switch to select a RADIUS server for authentication using Fabric Manager, follow these steps:

Step 1 Expand **Switches > Security > AAA,** and then select **RADIUS.**

You see the RADIUS configuration in the Information pane.

Step 2 Click the **Defaults** tab.

You see the RADIUS default settings.

Step 3 Check the **DirectedReq** check box for the RADIUS server.

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

About 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 seperator value *
```

Where **protocol** is a Cisco attribute for a particular type of authorization, **separator** is `=` (equal sign) for mandatory attributes, and `*` (asterisk) 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, such as authorization information, along with authentication results. This authorization information is specified through VSAs.

VSA Format

The following VSA protocol options are supported by the Cisco SAN-OS software:

- **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 by the Cisco SAN-OS software:

- **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. These are two examples using the roles attribute:

  ```
  shell:roles="network-admin vsan-admin"
  ```

  ```
  shell:roles*"network-admin vsan-admin"
  ```

  When an VSA is specified as **shell:roles*"network-admin vsan-admin"**, this VSA is flagged as an optional attribute, and other Cisco devices ignore this attribute.

- **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-related PDUs.

Specifying SNMPv3 on AAA Servers

The vendor/custom attribute **cisco-av-pair** can be used to specify user's role mapping using the format:

```
shell:roles="roleA roleB …"
```

If the roll option in the **cisco-av-pair** attribute is not set, the default user role is network-operator.

The VSA format optionally specifies your SNMPv3 authentication and privacy protocol attributes also as follows:

```
shell:roles="roleA roleB..." snmpv3:auth=SHA priv=AES-128
```

The SNMPv3 authentication protocol options are SHA and MD5. The privacy protocol options are AES-128 and DES. If these options are not specified in the **cisco-av-pair** attribute on the ACS server, MD5 and DES are used by default.

Configuring TACACS+ Server Monitoring Parameters

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 includes the following topics:

About TACACS+

TACACS+ is a client/server protocol that uses TCP (TCP port 49) for transport requirements. All switches in the Cisco MDS 9000 Family provide centralized authentication using the TACACS+ protocol. The TACACS+ has the following advantages over RADIUS authentication:

- Provides independent, modular AAA facilities. Authorization can be done without authentication.
- Uses the TCP transport protocol to send data between the AAA client and server, making 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.

About TACACS+ Server Default Configuration

Fabric Manager allows you to set up a default configuration that can be used for any TACACS+ server that you configure the switch to communicate with. The default configuration includes:

- Encryption type
- Preshared key

- Timeout value
- Number of retransmission attempts
- Allowing the user to specify a TACACS+ server at login

About the Default TACACS+ Server Encryption Type and Preshared Key

You need to configure the TACACS+ preshared key to authenticate the switch to the TACACS+ server. The length of the key is restricted to 64 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global key to be used for all TACACS+ server configurations on the switch.

You can override this global key assignment by explicitly using the **key** option when configuring and individual TACACS+ server.

Setting the Default TACACS+ Server Encryption Type and Preshared Key

To configure the default TACACS+ server encryption type and preshared key using Fabric Manager, follow these steps:

Step 1 Expand **Switches > Security > AAA,** and then select **TACACS+.**

You see the TACACS+ configuration in the Information pane.

Step 2 If the Defaults tab is dimmed, click the **CFS** tab.

Step 3 Click the **Defaults** tab.

You see the TACACS+ default settings.

Step 4 Select **plain** or **encrypted** from the AuthType drop-down menu and set the key in the Auth Key field.

Step 5 Click the **Apply Changes** icon to save the changes.

Setting the Default TACACS+ Server Timeout Interval and Retransmits

By default, a switch retries a TACACS+ server only once. This number can be configured. The maximum is five retries per server. You can also configure the timeout value for the TACACS+ server.

To configure the number of retransmissions and the time between retransmissions to the TACACS+ servers using Fabric Manager, follow these steps:

Step 1 Expand **Switches > Security > AAA,** and then select **TACACS+.**

You see the TACACS+ configuration in the Information pane.

Step 2 Choose the **Defaults** tab. (If the **Defaults** tab is disabled, click the **CFS** tab first.)

You see the TACACS+ default settings.

Step 3 Supply values for the Timeout and Retransmits fields for authentication attempts.

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

About TACACS+ Servers

By default, the TACACS+ feature is disabled in all switches in the Cisco MDS 9000 Family. Fabric Manager or Device Manager enables the TACACS+ feature automatically when you configure a TACACS+ server.

If a secret key is not configured for a configured server, a warning message is issued if a global key is not configured. If a server key is not configured, the global key (if configured) is used for that server.

Note Prior to Cisco MDS SAN-OS Release 2.1(2), you can use the dollar sign ($) in the key but the key must be enclosed in double quotes, for example “k$”. The percent sign (%) is not allowed. In Cisco MDS SAN-OS Release 2.1(2) and later, you can use the dollar sign ($) without double quotes and the percent sign (%) in global secret keys.

You can configure global values for the secret key for all TACACS+ servers.

Note If secret keys are configured for individual servers, those keys override the globally configured key.

Configuring a TACACS+ Server

To configure a TACACS+ server and all its options using Fabric Manager, follow these steps:

Step 1 Expand **Switches > Security > AAA,** and then select **TACACS+**.

You see the TACACS+ configuration in the Information pane.

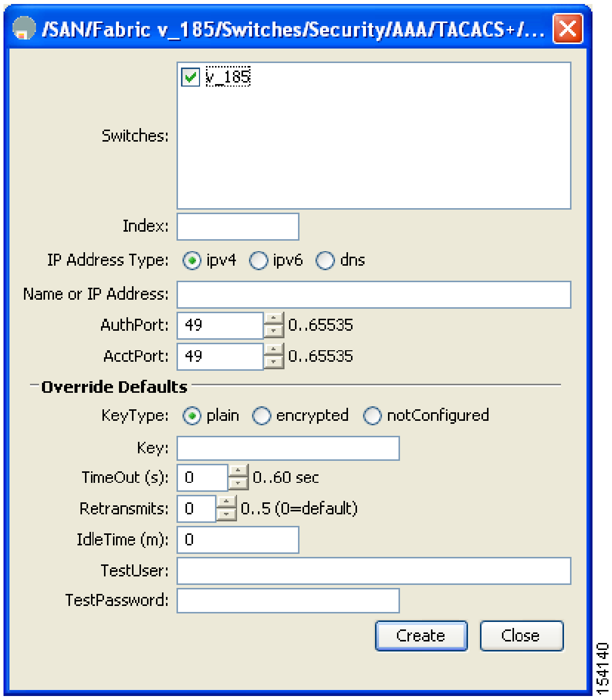
Step 2 Choose the **Servers** tab.

You see any existing TACACS+ servers.

Step 3 Click **Create Row** to add a new TACACS+ server.

You see the Create TACACS+ Server dialog box as shown in Figure 41-5.

Figure 41-5 Create TACACS+ Server Dialog Box



/SAN/Fabric v_185/Switches/Security/AAA/TACACS+/...

Switches: ☑ v_185

Index:

IP Address Type: ● ipv4 ○ ipv6 ○ dns

Name or IP Address:

AuthPort: 49 0..65535

AcctPort: 49 0..65535

Override Defaults

KeyType: ● plain ○ encrypted ○ notConfigured

Key:

TimeOut (s): 0 0..60 sec

Retransmits: 0 0..5 (0=default)

IdleTime (m): 0

TestUser:

TestPassword:

Create Close

Step 4 Select the switches that you want to assign as TACACS servers.

Step 5 Assign an index number to identify the TACACS server.

Step 6 Select the IP address type for the TACACS server.

Step 7 Fill in the IP address or name for the TACACS server.

Step 8 Modify the authentication and accounting ports used by this TACACS server.

Step 9 Select the appropriate key type for the TACACS server.

Step 10 Select the TimeOut value in seconds. The valid range is 0 to 60 seconds.

Step 11 Select the number of times the switch tries to connect to a TACACS server(s) before reverting to local authentication.

Step 12 Enter the test idle time interval value in minutes. The valid range is 1 to 1440 minutes.

Step 13 Enter the test user with the default password. The default username is test.

Step 14 Click **Create** to save these changes.

About Validating a TACACS+ Server

As of Cisco SAN-OS Release 3.0(1), you can periodically validate a TACACS+ server. The switch sends a test authentication to the server using the test username and test password that you configure. If the server does not respond to the test authentication, then the server is considered nonresponding.

Note We recommend that you do not configure the test user on your TACACS+ server for security reasons.

You can configure this option to test the server periodically, or you can run a one-time only test.

Periodically Validating a TACACS+ Server

To configure the switch to periodically test a TACACS+ server using Fabric Manager, see the "Configuring TACACS+ Server Monitoring Parameters" section on page 41-14.

Displaying TACACS+ Server Statistics

To display TACACS+ server statistics using Fabric Manager, follow these steps:

Step 1 Expand **Switches** > **Security** > **AAA,** and then select **TACACS+**.

You see the TACACS+ configuration in the Information pane.

Step 2 Choose the **Statistics** tab.

You see the TACACS+ server statistics.

About Users Specifying a TACACS+ Server at Login

By default, an MDS switch forwards an authentication request to the first server in the TACACS+ server group. You can configure the switch to allow the user to specify which TACACS+ server to send the authenticate request. If you enable this feature, the user can log in as *username@hostname*, where the *hostname* is the name of a configured TACACS+ server.

Allowing Users to Specify a TACACS+ Server at Login

To configure the switch to allow users to specify a TACACS+ server at login using Fabric Manager, follow these steps:

Step 1 Expand **Switches** > **Security** > **AAA,** and then select **TACACS+.**

You see the TACACS+ configuration in the Information pane.

Step 2 Click the **Defaults** tab.

You see the TACACS+ default settings.

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

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

About Custom Attributes for Roles

Cisco MDS 9000 Family switches use the TACACS+ custom attribute for service shells to configure roles to which a user belongs. TACACS+ attributes are specified in **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”
```

You can also configure optional custom attributes to avoid conflicts with non-MDS Cisco switches using the same AAA servers.

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

Additional custom attribute shell:roles are also supported:

```
shell:roles="network-admin vsan-admin"
```

or

```
shell:roles*"network-admin vsan-admin”
```

Note TACACS+ custom attributes can be defined on an Access Control Server (ACS) for various services (for example, shell). Cisco MDS 9000 Family switches require the TACACS+ custom attribute for the service shell to be used for defining roles.

Supported TACACS+ Servers

The Cisco SAN-OS software currently supports the following parameters for the listed TACACS+ servers:

- TACACS+

  ```
  cisco-av-pair=shell:roles="network-admin"
  ```

- Cisco ACS TACACS+

  ```
  shell:roles="network-admin"
  shell:roles*"network-admin"
  cisco-av-pair*shell:roles="network-admin"
  cisco-av-pair*shell:roles*"network-admin"
  cisco-av-pair=shell:roles*"network-admin"
  ```

- Open TACACS+

  ```
  cisco-av-pair*shell:roles="network-admin"
  cisco-av-pair=shell:roles*"network-admin"
  ```

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.

The AAA server monitoring feature can mark an AAA server as dead. You can configure a period of time in minutes to elapse before the switch sends requests to a dead AAA server. (See the "AAA Server Monitoring" section on page 41-5.)

This section includes the following topics:

- About Configuring Server Groups, page 41-20
- Configuring Server Groups, page 41-20

About Configuring Server Groups

You can configure these server groups at any time but they only take effect when you apply them to an AAA service. You configure AAA policies for CLI users or Fabric Manager or Device Manager users.

Configuring Server Groups

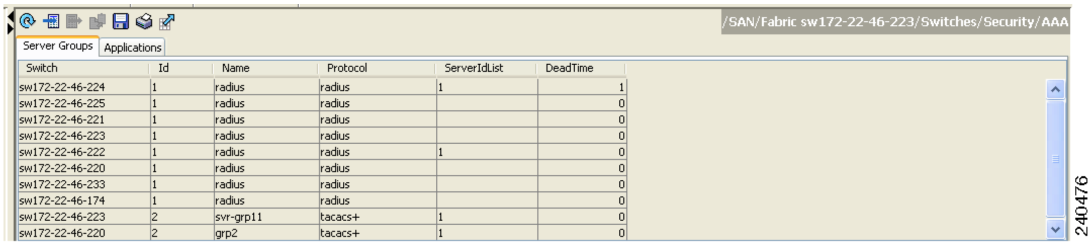
To configure a RADIUS or TACACS+ server group using Fabric Manager, follow these steps:

Step 1 Expand **Switches > Security,** and then select **AAA**.

You see the AAA configuration in the Information pane shown in Figure 41-6. If you do not see the screen in Figure 41-6, click the **Server Groups** tab.

You see the RADIUS or TACACS+ server groups configured.

Figure 41-6 AAA Server Groups



Switch	Id	Name	Protocol	ServerIdList	DeadTime
sw172-22-46-224	1	radius	radius	1	1
sw172-22-46-225	1	radius	radius		0
sw172-22-46-221	1	radius	radius		0
sw172-22-46-223	1	radius	radius		0
sw172-22-46-222	1	radius	radius	1	0
sw172-22-46-220	1	radius	radius		0
sw172-22-46-233	1	radius	radius		0
sw172-22-46-174	1	radius	radius		0
sw172-22-46-223	2	svr-grp11	tacacs+	1	0
sw172-22-46-220	2	grp2	tacacs+	1	0

Step 2 Click **Create Row** to create a server group.

You see the Create Server dialog box.

Step 3 Select the **radius** radio button to add a RADIUS server group or select **tacacs+** to add a TACACS+ server group.

Step 4 Supply server names for the ServerIdList field.

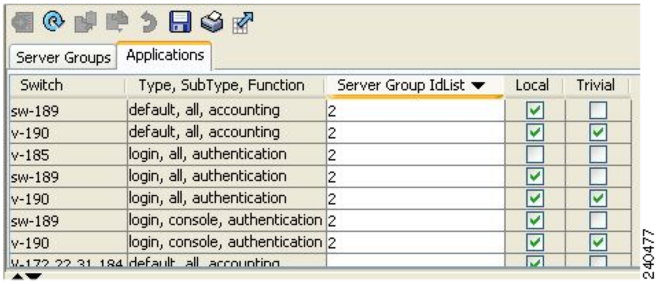
Step 5 Set the DeadTime field for the number of minutes that a server can be nonresponsive before it is marked as bypassed. See the "About Bypassing a Nonresponsive Server" section on page 41-21.

Step 6 Click **Create** to create this server group.

Step 7 Click the **Applications** tab to assign this server group to an application (see Figure 41-7).

You can associate a server group with all applications or you can specify certain applications.

Figure 41-7 Applications Tab



Switch	Type, SubType, Function	Server Group IdList	Local	Trivial
sw-189	default, all, accounting	2	☑	□
v-190	default, all, accounting	2	☑	☑
v-185	login, all, authentication	2	□	□
sw-189	login, all, authentication	2	☑	□
v-190	login, all, authentication	2	☑	☑
sw-189	login, console, authentication	2	☑	□
v-190	login, console, authentication	2	☑	☑
v-172.22.31.184	default, all, accounting		☑	□

Step 8 Click the **Apply Changes** icon to save the changes.

About Bypassing a Nonresponsive Server

As of Cisco SAN-OS Release 3.0(1), you can bypass a nonresponsive AAA server within a server group. If the switch detects a nonresponsive server, it will bypass that server when authenticating users. Use this feature to minimize login delays caused by a faulty server. Instead of sending a request to a nonresponsive server and waiting for the authentication request to timeout, the switch sends the authentication request to the next server in the server group. If there are no other responding servers in the server group, the switch continues to attempt authentications against the nonresponsive server.

AAA Server Distribution

Configuration for RADIUS and TACACS+ AAA on an MDS switch can be distributed using the Cisco Fabric Services (CFS). The distribution is disabled by default (see Chapter 13, "Using the CFS Infrastructure").

After enabling the distribution, the first server or global configuration starts an implicit session. All server configuration commands entered thereafter are stored in a temporary database and applied to all switches in the fabric (including the originating one) when you explicitly commit the database. The various server and global parameters are distributed, except the server and global keys. These keys are unique secrets to a switch and should not be shared with other switches.

Note Server group configurations are not distributed.

This section includes the following topics:

- Enabling AAA Server Distribution, page 41-22
- Starting a Distribution Session on a Switch, page 41-22
- Displaying the Session Status, page 41-23
- Displaying the Configuration to be Distributed, page 41-23
- Committing the Distribution, page 41-23
- Discarding the Distribution Session, page 41-23
- Clearing Sessions, page 41-24

- Merge Guidelines for RADIUS and TACACS+ Configurations, page 41-24

Note For an MDS switch to participate in AAA server configuration distribution, it must be running Cisco MDS SAN-OS Release 2.0(1b) or later.

Enabling AAA Server Distribution

Only switches where distribution is enabled can participate in the distribution activity.

To enable RADIUS server distribution using Fabric Manager, follow these steps:

Step 1 Expand **Switches > Security > AAA,**and then select **RADIUS**.

You see the RADIUS configuration in the Information pane.

Step 2 Click the **CFS** tab. You see the RADIUS CFS configuration.

Step 3 Choose **enable** from the Admin drop-down list for all switches that you want to enable CFS for RADIUS.

Step 4 Click **Apply Changes** to distribute these changes through the fabric.

.

To enable TACACS+ server distribution using Fabric Manager, follow these steps:

Step 1 Expand **Switches > Security > AAA,** and then select **TACACS+**.

You see the TACACS+ configuration in the Information pane.

Step 2 Choose the **CFS** tab.

You see the TACACS+ CFS configuration.

Step 3 Choose **enable** from the Admin drop-down list for all switches that you want to enable CFS on for TACACS+.

Step 4 Click **Apply Changes** to distribute these changes through the fabric.

.

Starting a Distribution Session on a Switch

A distribution session starts the moment you begin a RADIUS/TACACS+ server or global configuration. For example, the following tasks start an implicit session:

- Specifying the global timeout for RADIUS servers.
- Specifying the global timeout for TACACS+ servers.

Note After you issue the first configuration command related to AAA servers, all server and global configurations that are created (including the configuration that caused the distribution session start) are stored in a temporary buffer, not in the running configuration.

Displaying the Session Status

Once the implicit distribution session has started, you can check the session status from Fabric Manager by expanding **Switches > Security > AAA,** and selecting **RADIUS** or **TACACS+.** You see the **distribution status** on the CFS tab.

Displaying the Configuration to be Distributed

To display the RADIUS or TACACS+ global and/or server configuration stored in the temporary buffer using Fabric Manager, follow these steps:

Step 1 Expand **Switches > Security > AAA,** and then select **RADIUS** or select **TACACS+.**

Step 2 Click the CFS tab.

You see the distribution status on the CFS tab.

Step 3 Click the **pending** or **running** radio button.

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

Step 5 Click the **Servers** tab to view the pending or running configuration.

Committing the Distribution

The RADIUS or TACACS+ global and/or server configuration stored in the temporary buffer can be applied to the running configuration across all switches in the fabric (including the originating switch).

To distribute a RADIUS or TACACS+ configuration using Fabric Manager, follow these steps:

Step 1 Expand **Switches > Security > AAA,** and then select either **RADIUS** or **TACACS+**. You see the RADIUS or TACACS+ configuration in the Information pane.

Step 2 Choose the **CFS** tab. You see the RADIUS or TACACS+ CFS configuration.

Step 3 Choose **commitChanges** in the Config Action drop-down list for all switches that you want to enable CFS for RADIUS or TACACS+.

Step 4 Click **Apply Changes** to distribute the changes through the fabric.

.

Discarding the Distribution Session

Discarding the distribution of a session in progress causes the configuration in the temporary buffer to be dropped. The distribution is not applied.

To discard RADIUS or TACACS+ distribution using Fabric Manager, follow these steps:

Step 1 Expand **Switches > Security > AAA,** and then select either **RADIUS** or **TACACS+**. You see either the RADIUS or TACACS+ configuration in the Information pane.

Step 2 Click the **CFS** tab. You see either the RADIUS or TACACS+ CFS configuration.

Step 3 Choose **abort** from the Config Action drop-down list for each switch that should discard the pending RADIUS or TACACS+ distribution.

Step 4 Click **Apply Changes**.

.

Clearing Sessions

To clear a RADIUS or TACACS+ distribution using Fabric Manager, follow these steps:

Step 1 Expand **Switches > Security > AAA** and then select either **RADIUS** or **TACACS+**.

You see either the RADIUS or TACACS+ configuration in the Information pane.

Step 2 Choose the **CFS** tab. You see either the RADIUS or TACACS+ CFS configuration.

Step 3 Choose **clear** from the Config Action drop-down list for each switch that should clear the pending RADIUS or TACACS+ distribution.

Step 4 Click **Apply Changes**.

.

Merge Guidelines for RADIUS and TACACS+ Configurations

The RADIUS and TACACS+ server and global configuration are merged when two fabrics merge. The merged configuration is applied to CFS distribution-enabled switches.

When merging the fabric, be aware of the following conditions:

- The server groups are not merged.
- The server and global keys are not changed during the merge.
- The merged configuration contains all servers found on all CFS enabled switches.
- The timeout and retransmit parameters of the merged configuration are the largest values found per server and global configuration.

Caution If there is a conflict between two switches in the server ports configured, the merge fails.

MSCHAP Authentication

Microsoft Challenge Handshake Authentication Protocol (MSCHAP) is the Microsoft version of CHAP. You can use MSCHAP for user logins to an MDS switch through a remote authentication server (RADIUS or TACACS+).

About Enabling MSCHAP

By default, the switch uses Password Authentication Protocol (PAP) authentication between the switch and the remote server. If you enable MSCHAP, you need to configure your RADIUS server to recognize the MSCHAP vendor-specific attributes. See the "About Vendor-Specific Attributes" section on page 41-13. Table 41-1 shows the RADIUS vendor-specific attributes required for MSCHAP.

Table 41-1 MSCHAP RADIUS Vendor-Specific Attributes

Vendor-ID Number	Vendor-Type Number	Vendor-Specific Attribute	Description
311	11	MSCHAP-Challenge	Contains the challenge sent by an AAA server to an MSCHAP user. It can be used in both Access-Request and Access-Challenge packets.
211	11	MSCHAP-Response	Contains the response value provided by an MS-CHAP user in response to the challenge. It is only used in Access-Request packets.

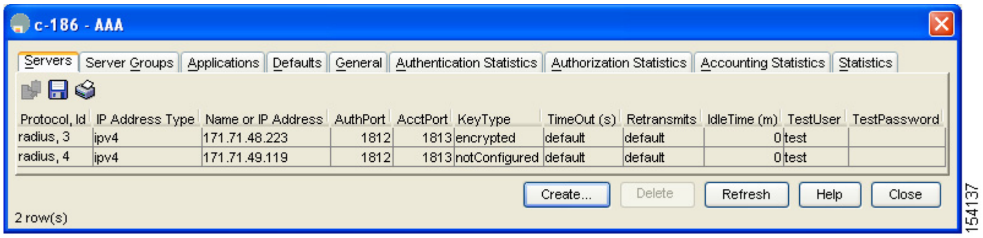
Enabling MSCHAP Authentication

To enable MSCHAP authentication using Device Manager, follow these steps:

Step 1 Click **Security > AAA.**

You see the AAA configuration in the Information pane as shown in Figure 41-8.

Figure 41-8 AAA Configuration in Device Manager



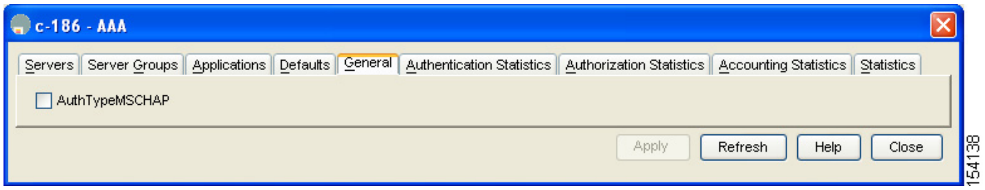
Protocol, Id	IP Address Type	Name or IP Address	AuthPort	AcctPort	KeyType	TimeOut (s)	Retransmits	IdleTime (m)	TestUser	TestPassword
radius, 3	ipv4	171.71.48.223	1812	1813	encrypted	default	default	0	test	
radius, 4	ipv4	171.71.49.119	1812	1813	notConfigured	default	default	0	test	

2 row(s)

Step 2 Click the **General** tab.

You see the MSCHAP configuration as shown in Figure 41-9.

Figure 41-9 MSCHAP Configuration



□ AuthTypeMSCHAP

Step 3 Check the **AuthTypeMSCHAP** check box to use MSCHAP to authenticate users on the switch.

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

.

Local AAA Services

The system maintains the username and password locally and stores the password information in encrypted form. You are authenticated based on the locally stored user information. See the "Configuring Roles and Profiles" section on page 39-2.

You can turn off password verification using the **none** option. If you configure this option, users can log in without giving a valid password. But the user should at least exist locally on the Cisco MDS 9000 Family switch.

Caution Use this option cautiously. If configured, any user can access the switch at any time.

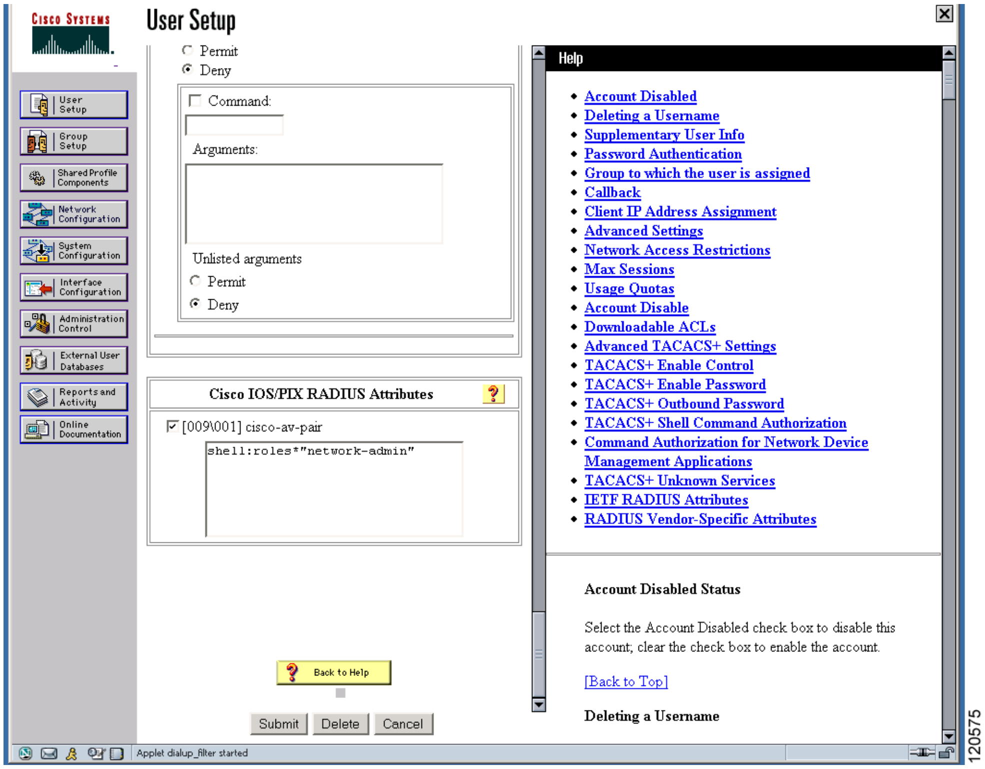
Refer to the *Cisco MDS 9000 Family CLI Configuration Guide* to configure this option.

Configuring Cisco Access Control Servers

The Cisco Access Control Server (ACS) uses TACACS+ and RADIUS protocols to provide AAA services that ensure a secure environment.When using the AAA server, user management is normally done using Cisco ACS. Figure 41-10, Figure 41-11, Figure 41-12, and Figure 41-13 display ACS server user setup configurations for network-admin roles and multiple roles using either RADIUS or TACACS+.

Caution Cisco MDS SAN-OS does not support all numeric usernames, whether created with RADIUS or TACACS+, or created locally. Local users with all numeric names cannot be created. If an all numeric user name exists on an AAA server and is entered during login, the user is not logged in.

Figure 41-10 Configuring the network-admin Role When Using RADIUS



User Setup

○ Permit
● Deny

□ Command:

Arguments:

Unlisted arguments
○ Permit
● Deny

Cisco IOS/PIX RADIUS Attributes

☑ [009\001] cisco-av-pair

```
shell:roles*"network-admin"
```

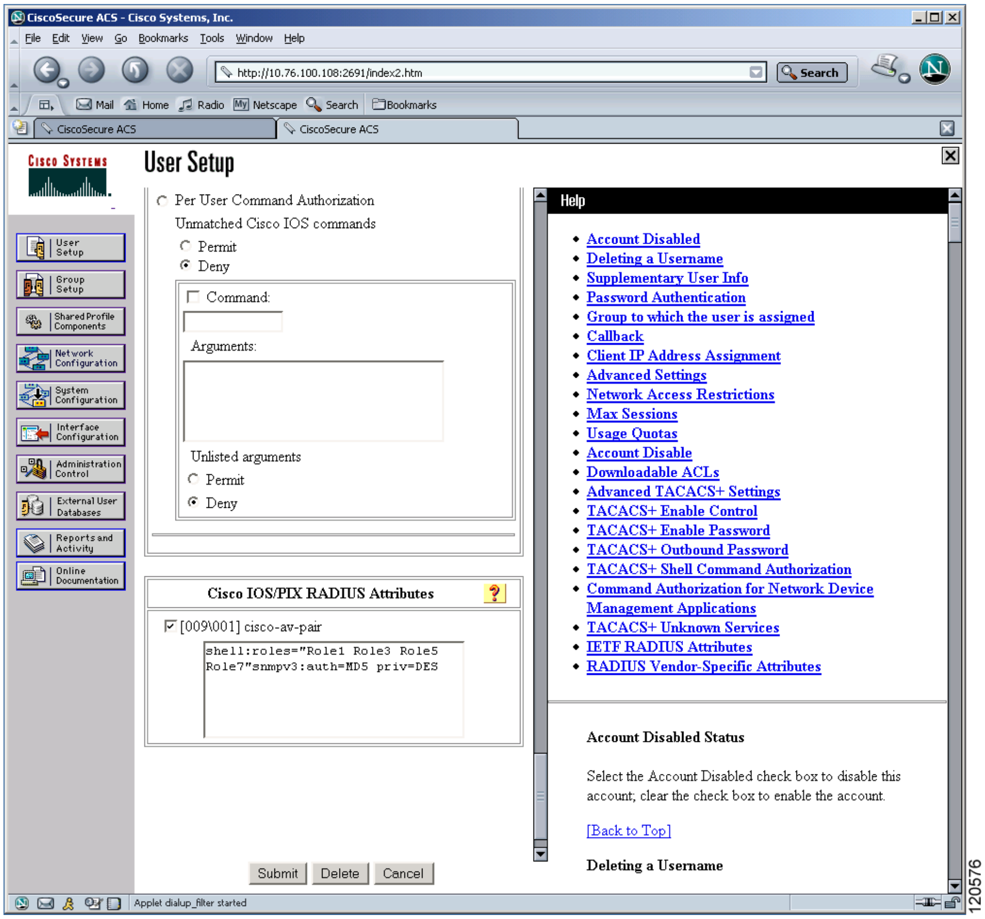
Account Disabled Status

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[Back to Top]

Deleting a Username

Figure 41-11 Configuring Multiple Roles with SNMPv3 Attributes When Using RADIUS



User Setup

○ Per User Command Authorization

Unmatched Cisco IOS commands

○ Permit

● Deny

□ Command:

Arguments:

Unlisted arguments

○ Permit

● Deny

Cisco IOS/PIX RADIUS Attributes

☑ [009\001] cisco-av-pair

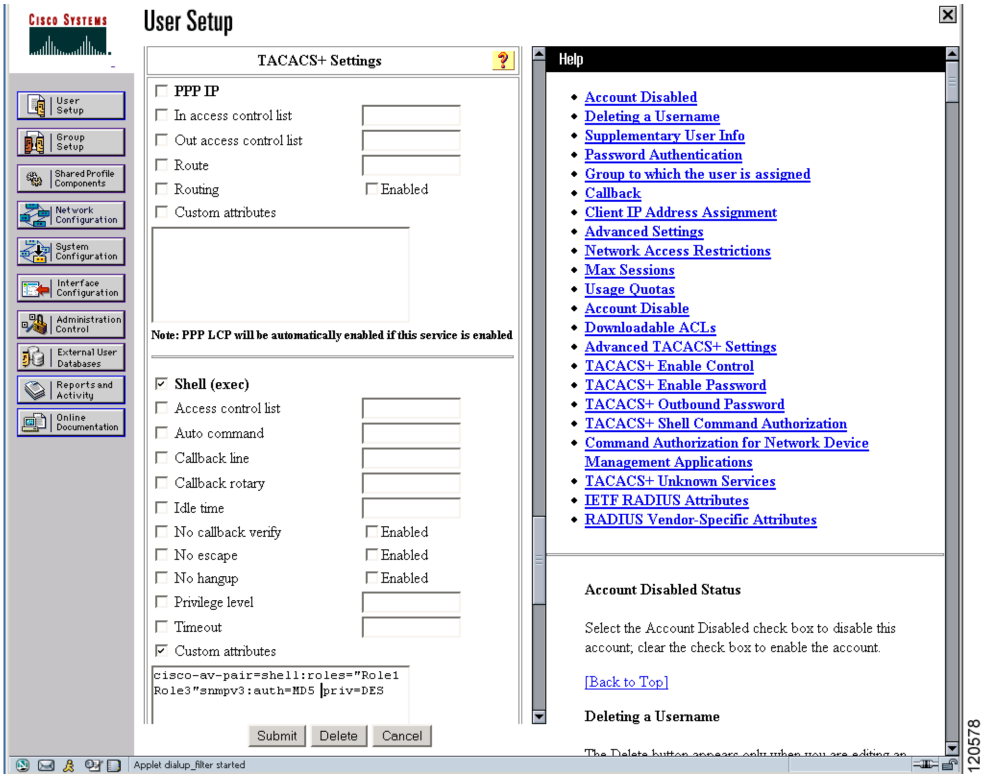
```
shell:roles="Role1 Role3 Role5
Role7"snmpv3:auth=MD5 priv=DES
```

Account Disabled Status

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

Deleting a Username

Figure 41-12 Configuring the network-admin Role with SNMPv3 Attributes When Using TACACS+



TACACS+ Settings

□ PPP IP
□ In access control list
□ Out access control list
□ Route
□ Routing □ Enabled
□ Custom attributes

Note: PPP LCP will be automatically enabled if this service is enabled

☑ Shell (exec)
□ Access control list
□ Auto command
□ Callback line
□ Callback rotary
□ Idle time
□ No callback verify □ Enabled
□ No escape □ Enabled
□ No hangup □ Enabled
□ Privilege level
□ Timeout
☑ Custom attributes

```
cisco-av-pair=shell:roles="Role1
Role3"snmpv3:auth=MD5 priv=DES
```

Help

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

Account Disabled Status

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

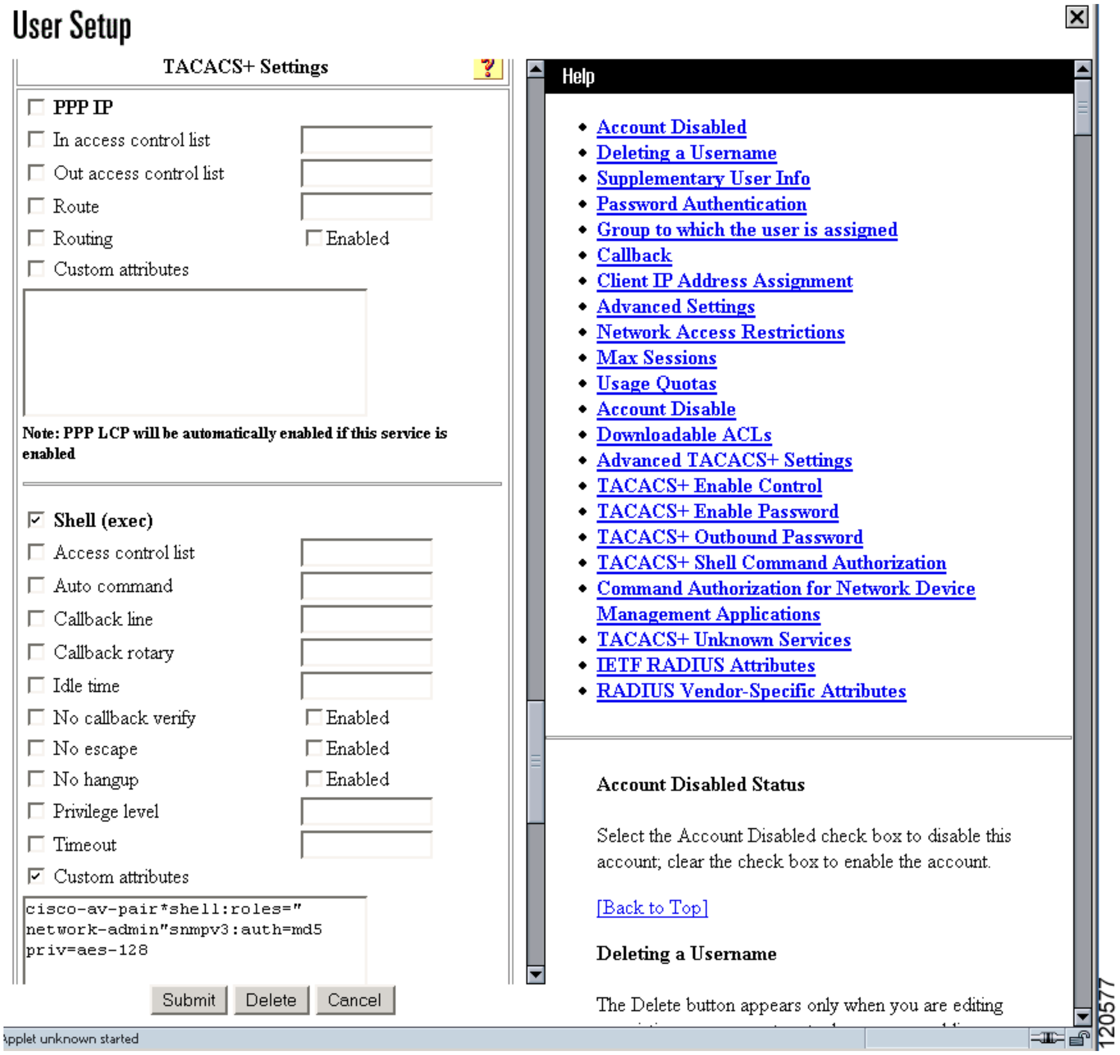
[Back to Top]

Deleting a Username

The Delete button appears only when you are editing an

Applet dialup_filter started

Figure 41-13 Configuring Multiple Roles with SNMPv3 Attributes When Using TACACS+



User Setup

TACACS+ Settings

□ PPP IP
□ In access control list
□ Out access control list
□ Route
□ Routing □ Enabled
□ Custom attributes

Note: PPP LCP will be automatically enabled if this service is enabled

☑ Shell (exec)
□ Access control list
□ Auto command
□ Callback line
□ Callback rotary
□ Idle time
□ No callback verify □ Enabled
□ No escape □ Enabled
□ No hangup □ Enabled
□ Privilege level
□ Timeout
☑ Custom attributes

```
cisco-av-pair*shell:roles="
network-admin"snmpv3:auth=md5
priv=aes-128
```

- Account Disabled
- Deleting a Username
- Supplementary User Info
- Password Authentication
- Group to which the user is assigned
- Callback
- Client IP Address Assignment
- Advanced Settings
- Network Access Restrictions
- Max Sessions
- Usage Quotas
- Account Disable
- Downloadable ACLs
- Advanced TACACS+ Settings
- TACACS+ Enable Control
- TACACS+ Enable Password
- TACACS+ Outbound Password
- TACACS+ Shell Command Authorization
- Command Authorization for Network Device Management Applications
- TACACS+ Unknown Services
- IETF RADIUS Attributes
- RADIUS Vendor-Specific Attributes

Account Disabled Status

Select the Account Disabled check box to disable this account; clear the check box to enable the account.

[Back to Top]

Deleting a Username

The Delete button appears only when you are editing

Default Settings

Table 41-2 lists the default settings for all switch security features in any switch.

Table 41-2 Default Switch Security Settings

Parameters	Default
Roles in Cisco MDS switches	Network operator (network-operator)
AAA configuration services	Local
Authentication port	1821
Accounting port	1813
Preshared key communication	Clear text

Table 41-2 Default Switch Security Settings (continued)

Parameters	**Default**
RADIUS server timeout	1 (one) second
RADIUS server retries	Once
RADIUS server directed requests	Disabled
TACACS+	Disabled
TACACS+ servers	None configured
TACACS+ server timeout	5 seconds
TACACS+ server directed requests	Disabled
AAA server distribution	Disabled
Accounting log size	250 KB