CHAPTER 29

Configuring Security Features on an External AAA Server

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 Remote Access Dial-In User Service (RADIUS) or Terminal Access Controller Access Control device Plus (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 topics:

Information About 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:

Security Options

You can access the CLI using the console (serial connection), Telnet, or Secure Shell (SSH). You can access DCNM-SAN using TCP/UDP SNMP or HTTP traffic. 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 the RADIUS, TACACS+, and LDAP Server" section on page 29-78
  - Using TACACS+

    See the "Configuring the RADIUS, TACACS+, and LDAP Server" section on page 29-78
- Local security control.

  See the "Local AAA Services" section on page 29-74.

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

- iSCSI authentication

See the *IP Services Configuration Guide, Cisco DCNM for SAN.*

- Fibre Channel Security Protocol (FC-SP) authentication

  See Chapter 31, "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 DCNM for SAN).

SNMP security options also apply to DCNM for SAN and Device Manager.

See the *Cisco MDS 9000 NX-OS Family System Management Configuration Guide* for more information on the SNMP security options.

Refer to the *Cisco DCNM Fundamentals Guide* for information on DCNM for SAN and Device Manager.

Switch AAA Functionalities

Using the CLI or DCNM for SAN (DCNM-SAN), or an SNMP application, you can configure AAA switch functionalities on any switch in the Cisco MDS 9000 Family.

This section includes the following topics:

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 DCNM-SAN 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 DCNM-SAN 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 (DCNM-SAN 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.

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 Service 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 (DCNM-SAN and Device Manager login)
- Console login
- iSCSI authentication (see the *IP Services Configuration GuideCisco MDS 9000 Family NX-OS IP Services Configuration Guide*, *Cisco DCNM for SAN*).
- FC-SP authentication (see Chapter 31, “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 NX-OS supports user names that are created with alphanumeric characters or specific special characters (+ [plus], = [equal], _ [underscore], - [hyphen] , \ [backslash], and . [period]) whether created remotely (using TACACS+ or RADIUS) or locally, provided the user name starts with an alphabetical character. Local user names cannot be created with all numbers or with any special characters (apart from those specified). If a numeric-only user name or a non-supported special character user name exists on an AAA server, and is entered during login, then the user is denied access.

Note Even if local is not specified as one of the options, it is tried by default if all AAA servers configured for authentication are unreachable. User has the flexibility to disable this fallback (See section “Configuring Fallback Mechanism for Authentication” section on page 29-81).

When RADIUS times out, local login is attempted depending on the fallback configuration. 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.

Table 29-1 provides the related CLI command for each AAA service configuration option.

Table 29-1 AAA Service Configuration Commands

AAA Service Configuration Option	Related Command
Telnet or SSH login (Cisco DCNM-SAN and Device Manager login)	**aaa authentication login default**
Console login	**aaa authentication login console**
iSCSI authentication	**aaa authentication iscsi default**
FC-SP authentication	**aaa authentication dhchap default**
Accounting	**aaa accounting default**

Error-Enabled Status

When you log in, the login is processed by rolling over to local user database if the remote AAA servers do not respond. In this situation, the following message is displayed on your screen if you have enabled the error-enabled feature:

```
Remote AAA servers unreachable; local authentication done.
```

To enable this message display, use the **aaa authentication login error-enable** command.

To disable this message display, use the **no aaa authentication login error-enable** command.

To view the current display status, use the **show aaa authentication login error-enable** command (see Example 29-1).

Example 29-1 Displays AAA Authentication Login Information

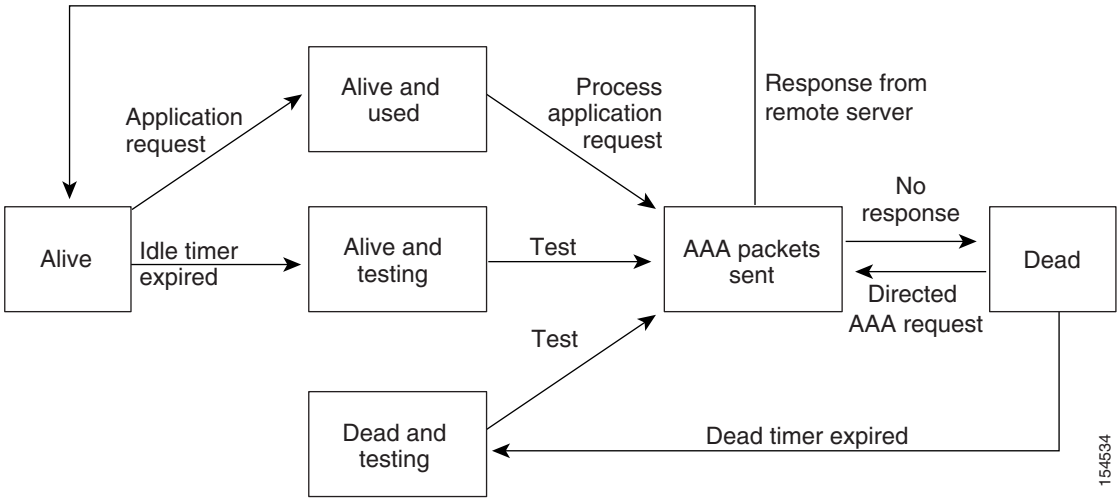
```
switch# show aaa authentication login error-enable
enabled
```

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 29-1 for AAA server states.

Figure 29-1 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 the RADIUS, TACACS+, and LDAP Server" section on page 29-78 and"Displaying RADIUS Server Details" section on page 29-119.

Authentication and Authorization Process

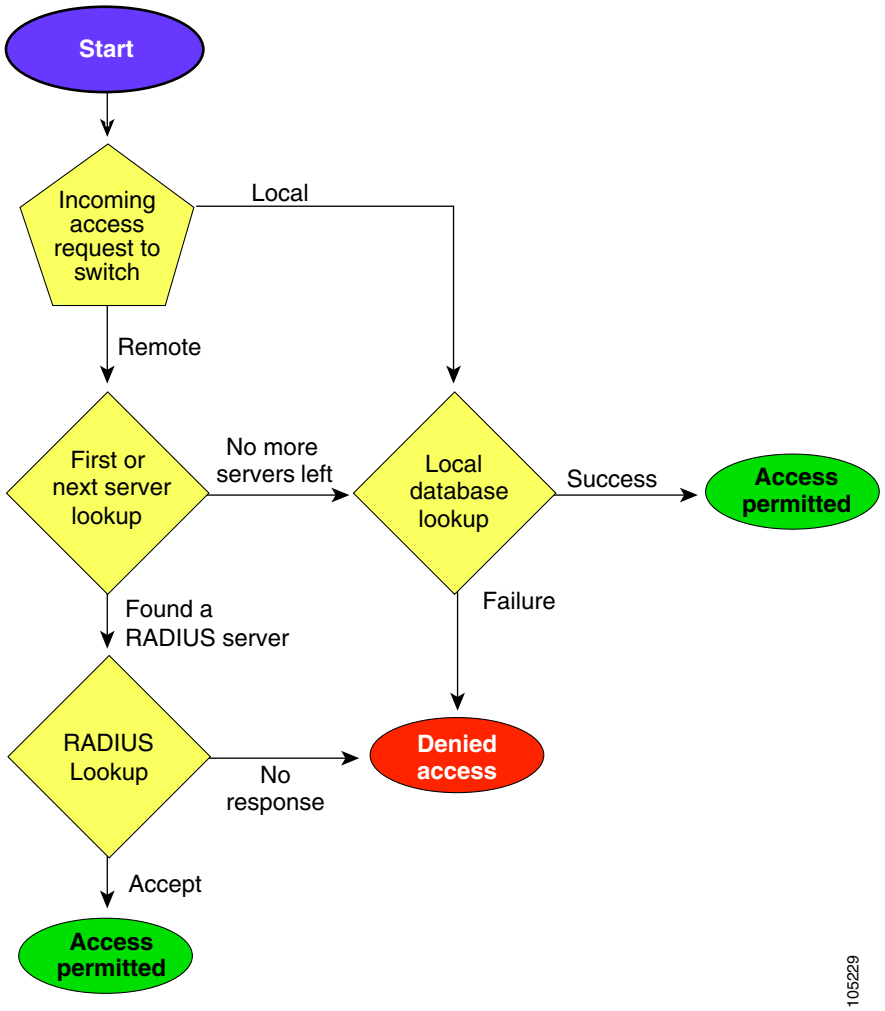
Authentication is the process of verifying the identity of the person managing the switch. This identity verification is based on the user ID and password combination provided by the person managing the switch. The Cisco MDS 9000 Family switches allow you to perform local authentication (using the lookup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

Authorization provides access control. It is the process of assembling a set of attributes that describe what the user is authorized to perform. Based on the user ID and password combination, the user is authenticated and authorized to access the network as per the assigned role. You can configure parameters that can prevent unauthorized access by an user, provided the switches use the TACACS+ protocol.

AAA authorization is the process of assembling a set of attributes that describe what the user is authorized to perform. Authorization in the Cisco NX-OS software is provided by attributes that are downloaded from AAA servers. Remote security servers, such as RADIUS and TACACS+, authorize users for specific rights by associating attribute-value (AV) pairs, which define those rights with the appropriate user.

Figure 29-2 shows a flow chart of the authorization and authentication process.

Figure 29-2 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.

Global AAA Server Monitoring Parameters

The global AAA server monitoring parameters function as follows:

- When a new AAA server is configured it is monitored using the global test parameters, if defined.
- When global test parameters are added or modified, all the AAA servers, which do not have any test parameters configured, start getting monitored using the new global test parameters.
- When the server test parameters are removed for a server or when the idle-time is set to zero (default value) the server starts getting monitored using the global test parameters, if defined.
- If global test parameters are removed or global idle-time is set to zero, servers for which the server test parameters are present are not affected. However, monitoring stops for all other servers that were previously being monitored using global parameters.

- If the server monitoring fails with the user-specified server test parameters, the server monitoring does not fall back to global test parameters.

LDAP

The Lightweight Directory Access Protocol (LDAP) provides centralized validation of users attempting to gain access to a Cisco NX-OS device. LDAP services are maintained in a database on an LDAP daemon running, typically, on a UNIX or Windows NT workstation. You must have access to and must configure an LDAP server before the configured LDAP features on your Cisco NX-OS device are available.

LDAP provides for separate authentication and authorization facilities. LDAP allows for a single access control server (the LDAP daemon) to provide each service-authentication and authorization-independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.

The LDAP client/server protocol uses TCP (TCP port 389) for transport requirements. Cisco NX-OS devices provide centralized authentication using the LDAP protocol.

Note If you are familiar with the Cisco IOS CLI, be aware that the Cisco NX-OS commands for this feature might differ from the Cisco IOS commands that you would use.

LDAP Authentication and Authorization

Clients establish a TCP connection and authentication session with an LDAP server through a simple bind (username and password). As part of the authorization process, the LDAP server searches its database to retrieve the user profile and other information.

You can configure the bind operation to first bind and then search, where authentication is performed first and authorization next, or to first search and then bind. The default method is to first search and then bind.

The advantage of searching first and binding later is that the distinguished name (DN) received in the search result can be used as the user DN during binding rather than forming a DN by prepending the username (cn attribute) with the baseDN. This method is especially helpful when the user DN is different from the username plus the baseDN. For the user bind, the bindDN is constructed as baseDN + append-with-baseDN, where append-with-baseDN has a default value of cn=$userid.

Note As an alternative to the bind method, you can establish LDAP authentication using the compare method, which compares the attribute values of a user entry at the server. For example, the user password attribute can be compared for authentication. The default password attribute type is userPassword.

About RADIUS Server Default Configuration

DCNM-SAN 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 serverin the **radius-server host** command.

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 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.

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.

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.

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 separator 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 NX-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 NX-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 role 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.

One-Time Password Support

A one-time password (OTP) is a password that is valid for a single login session or transaction. OTPs avoid a number of shortcomings that are associated with usual (static) passwords. The most vital shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not at risk to replay attacks. If an intruder manages to record an OTP that was already used to log into a service or to conduct an operation, it will not be misused because it is no longer valid.

One-time password applies only to RADIUS and TACACS protocol daemons. In the case of the RADIUS protocol daemon, there is no configuration required from the switch side. In the case of the TACACS protocol, ASCII authentication mode needs to be enabled using the following command.

```
aaa authentication login ascii-authentication
```

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

DCNM-SAN 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 an individual TACACS+ server.

About TACACS+ Servers

By default, the TACACS+ feature is disabled in all switches in the Cisco MDS 9000 Family. DCNM-SAN 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.

Password Aging Notification through TACACS+ Server

Password aging notification is initiated when the user authenticates to a Cisco MDS 9000 switch via a TACACS+ account. The user is notified when a password is about to expire or has expired. If the password has expired, user is prompted to change the password.

Note As of Cisco MDS SAN-OS Release 3.2(1), only TACACS+ supports password aging notification. If you try to use RADIUS servers by enabling this feature, RADIUS generates a SYSLOG message and authentication falls back to the local database.

Password aging notification facilitates the following:

- Password change—You can change your password by entering a blank password.
- Password aging notification—Notifies password aging. Notification happens only if the AAA server is configured and MSCHAP and MSCHAPv2 is disabled.
- Password change after expiration—Initiates password change after the old password expires. Initiation happens from the AAA server.

Note Password aging notification fails if you do not disable MSCHAP and MSCHAPv2 authentication.

To enable the password aging option in the AAA server, enter the following command:

```
aaa authentication login ascii-authentication
```

To determine whether or not password aging notification is enabled or disabled in the AAA server, enter the following command:

```
show aaa authentication login ascii-authentication
```

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 DCNM-SAN, see the "Configuring the RADIUS, TACACS+, and LDAP Server" section on page 29-78.

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.

Supported TACACS+ Server Parameters

The Cisco NX-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"
```

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 the *Cisco MDS 9000 Family NX-OS System Management Configuration GuideSystem Management Configuration Guide, Cisco DCNM for SAN*).

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.

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, or Cisco NX-OS Release 4.1(1).

Starting a Distribution Session on a Switch

A distribution session starts the moment you begin a RADIUS or 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.

CHAP Authentication

Challenge Handshake Authentication Protocol (CHAP) is a challenge-response authentication protocol that uses the industry-standard Message Digest 5 (MD5) hashing scheme to encrypt the response. CHAP is used by various vendors of network access servers and clients. A server running routing and remote access supports CHAP so that remote access clients that require CHAP are authenticated. CHAP is supported as an authentication method in this release.

MSCHAP Authentication

Microsoft Challenge Handshake Authentication Protocol (MSCHAP) is the Microsoft version of CHAP.

Cisco MDS 9000 Family switches allow user logins to perform remote authentication using different versions of MSCHAP. MSCHAP is used for authentication on a RADIUS or TACACS+ server, while MSCHAPv2 is used for authentication on a RADIUS server.

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 29-69. Table 29-2 shows the RADIUS vendor-specific attributes required for MSCHAP.

Table 29-2 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.

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.

Accounting Services

Accounting refers to the log information that is kept for each management session in a switch. This information may be used to generate reports for troubleshooting and auditing purposes. Accounting can be implemented locally or remotely (using RADIUS). The default maximum size of the accounting log is 250,000 bytes and cannot be changed.

Tip The Cisco MDS 9000 Family switch uses interim-update RADIUS accounting-request packets to communicate accounting log information to the RADIUS server. The RADIUS server must be appropriately configured to log the information communicated in these packets. Several servers typically have log update/watchdog packets flags in the AAA client configuration. Turn on this flag to ensure proper RADIUS accounting.

Note Configuration operations are automatically recorded in the accounting log if they are performed in configuration mode. Additionally, important system events (for example, configuration save and system switchover) are also recorded in the accounting log.

Defining Roles on the Cisco Secure ACS 5.x GUI

Enter the following in the GUI under **Policy Elements**:

Table 29-3 Role Definitions

Attribute	Requirement	Value
shell:roles	Optional	network-admin

Defining 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.

Guidelines and Limitations

This section has the following topics:

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 the *IP Services Configuration Guide, Cisco DCNM for SANCisco MDS 9000 Family NX-OS Configuration Guide*). 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.

Guidelines and Limitations for LDAP

LDAP has the following guidelines and limitations:

- You can configure a maximum of 64 LDAP servers on the Cisco NX-OS device.
- Cisco NX-OS supports only LDAP version 3.
- Cisco NX-OS supports only these LDAP servers:
  - OpenLDAP
  - Microsoft Active Directory
- LDAP over Secure Sockets Layer (SSL) supports only SSL version 3 and Transport Layer Security (TLS) version 1.
- If you have a user account configured on the local Cisco NX-OS device that has the same name as a remote user account on an AAA server, the Cisco NX-OS software applies the user roles for the local user account to the remote user, not the user roles configured on the AAA server.

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.

Note Test parameter will be distributed via CFS for TACACS+ Daemon only. If the fabric contains only Cisco NX-OS Release 5.0 devices, then the test parameters will be distributed. If the fabric contains devices running Release 5.0 and some running Release 4.x, the test parameters are not distributed.

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

Default Settings

Table 29-4 lists the default settings for LDAP parameters.

Table 29-4 Default LDAP Parameter Settings

Parameters	Default
LDAP	Disabled
LDAP authentication method	First search and then bind
LDAP authentication mechanism	Plain
Dead-interval time	0 minutes
Timeout interval	5 seconds
Idle timer interval	60 minutes
Periodic server monitoring username	test
Periodic server monitoring password	Cisco

Table 29-5 lists the default settings for all switch security features in any switch.

Table 29-5 Default Switch Security Settings

Parameters	Default
Roles in Cisco MDS switches	Network operator (network-operator)
AAA configuration services	Local
Authentication port	1812
Accounting port	1813
Preshared key communication	Clear text
RADIUS server timeout	1 (one) second
RADIUS server retries	Once
Authorization	Disabled
aaa user default role	enabled
RADIUS server directed requests	Disabled
TACACS+	Disabled

Table 29-5 Default Switch Security Settings (continued)

Parameters	Default
TACACS+ servers	None configured
TACACS+ server timeout	5 seconds
TACACS+ server directed requests	Disabled
AAA server distribution	Disabled
Accounting log size	250 KB

Configuring the RADIUS, TACACS+, and LDAP Server

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.

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:

Authorizing and Authenticating the Switch

To authorize and authenticate the switch, follow these steps:

Step 1 Log in to the required switch in the Cisco MDS 9000 Family, using the Telnet, SSH, DCNM-SAN or 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 by default local database is used for authentication. The next section will describe the way to disable this fallback.

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 if the **show aaa user default-role** command is enabled. You are denied access if this command is disabled.

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.

Configuring Role-based Authorization on TACACS+ Server

To configure role-based authorization on TACACS+ server, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# aaa authorization`	Enables configuration of authorization methods.
Step 3	`switch(config)# aaa authorization config-commands`	Enables authorization for all commands under config mode Layer2 and Layer3.
Step 4	`switch(config)# aaa authorization config-commands default group tac1`	Enables specified TACACS+ server group authorization.
Step 5	`switch(config)# aaa authorization commands`	Enables AAA authorization for all EXEC mode commands.
Step 6	`switch(config)# aaa authorization commands default group tac1`	Enables specified TACACS+ server group authorization.
Step 7	`switch(config)# aaa authorization commands default group local`	Enables default TACACS+ server group authorization.Authorization is based on the local-user-database.
Step 8	`switch(config)# no aaa authorization command default group tac1`	Removes authorization for a specified function for the authenticated user.

Note Authorization configuration is provided only for authentication done using TACACS+ server.

Note The ‘none’ option from aaa authorization methods has been deprecated. If you did an upgrade from 4.x image and ‘none’ was configured as one of the authorization methods, it is be replaced with local. The functionality remains the same.

Configuring Fallback Mechanism for Authentication

You can enable or disable fallback to the local database in case the remote authentication is set and all of the AAA servers are unreachable (authentication error). The fallback is set to local by default in case of an authentication error. You can disable this fallback for both console and SSH or Telnet login. Disabling this fallback tightens the authentication security.

To configure the fallback mechanism, follow this step:

Step 1 Enter the **show run aaa all** command to verify that the default fallback is enabled for both the default and console login.

Disabling fallback will print a warning message.

The CLI syntax and behavior is as follows:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.

Step 2	`switch(config)# sh run aaa all`
	`aaa authentication login default fallback error local`
	`aaa authentication login console fallback error local`
		Displays the default fallback behavior.

Step 3	`switch(config)# no aaa authentication login default fallback error local` `WARNING!!! Disabling fallback can lock your switch.`	Disables the fallback to local database for authentication. **Note** Replace **default** with **console** in this command to disable fallback to console.

Caution If fallback is disabled for both the default and console, remote authentication is enabled and servers are unreachable and then the switch will be locked.

Configuring AAA Server Monitoring Parameters Globally

The AAA server monitoring parameters can be configured globally for all servers or individually for a specific server. This section explains how the global configuration can be set. The global configurations will apply to all servers that do not have individual monitoring parameters defined. For any server, the individual test parameter defined for that particular server will always get precedence over the global settings.

Use the following commands to configure the global monitoring parameters for RADIUS servers:

	Command	Purpose
Step 1	`switch# config t` `switch(config)#`	Enters configuration mode.
Step 2	`switch(config)# radius-server deadtime 10`	Sets global deadtime for RADIUS servers to 10 minutes. Acceptable Range: 0 to 1440 minutes.
Step 3	`switch(config)# radius-server timeout 20f`	Sets global timeout for RADIUS servers to 20 seconds. Acceptable Range: 1 to 60 seconds.
Step 4	`switch(config)# radius-server retransmit 2`	Sets global retransmit count for RADIUS servers to 2. Acceptable Range 0 to 5
Step 5	`switch(config)# radius-server test username username password password idle-time time`	Globally configures test parameters for the RADIUS servers.
	`switch(config)# radius-server test username username password password no`	Disables global test parameters for the RADIUS servers.

Note Replace “radius” with “tacacs” in the steps above to get equivalent commands for TACACS server global test parameter configurations.

Enabling LDAP

By default, the LDAP feature is disabled on the Cisco NX-OS device. You must explicitly enable the LDAP feature to access the configuration and verification commands for authentication.

Prerequisites

LDAP has the following prerequisites:

- Obtain the IPv4 or IPv6 addresses or hostnames for the LDAP servers.
- Ensure that the Cisco NX-OS device is configured as an LDAP client of the AAA servers.

To enable LDAP, follow these steps:

	Command	Purpose
Step 1	`switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	`switch(config)# feature ldap`	Enables LDAP.

	Command	Purpose
Step 3	`switch(config)# exit` `switch#`	Exits configuration mode.
Step 4	`switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring LDAP Server Hosts

To access a remote LDAP server, you must configure the IP address or the hostname for the LDAP server on the Cisco NX-OS device. You can configure up to 64 LDAP servers.

Note By default, when you configure an LDAP server IP address or hostname on the Cisco NX-OS device, the LDAP server is added to the default LDAP server group. You can also add the LDAP server to another LDAP server group.

To configure LDAP server hosts, follow these steps:

	Command	Purpose
Step 1	`switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	`switch(config)# ldap-server host 10.10.2.2 enable-ssl`	Specifies the IPv4 or IPv6 address or hostname for an LDAP server. The **enable-ssl** keyword ensures the integrity and confidentiality of the transferred data by causing the LDAP client to establish a Secure Sockets Layer (SSL) session prior to sending the bind or search request.
Step 3	`switch(config)# exit` `switch#`	Exits configuration mode.
Step 4	`switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring the RootDN for an LDAP Server

You can configure the root designated name (DN) for the LDAP server database. The rootDN is used to bind to the LDAP server to verify its state.

To configure the RootDN for an LDAP server, follow these steps:

	Command	Purpose
Step 1	`switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	`switch(config)# ldap-server host 10.10.1.1 rootDN cn=manager,dc=acme,dc=com password Ur2Gd2BH timeout 60`	Specifies the rootDN for the LDAP server database and the bind password for the root. Optionally specifies the TCP port to use for LDAP messages to the server. The range is from 1 to 65535, and the default TCP port is the global value or 389 if a global value is not configured. Also specifies the timeout interval for the server. The range is from 1 to 60 seconds, and the default timeout is the global value or 5 seconds if a global value is not configured.
Step 3	`switch(config)# exit` `switch#`	Exits configuration mode.
Step 4	`switch# show ldap-server`	(Optional) Displays the LDAP server configuration.
Step 5	`switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring LDAP Server Groups

You can specify one or more remote AAA servers to authenticate users using server groups. All members of a group must be configured to use LDAP. The servers are tried in the same order in which you configure them.

You can configure these server groups at any time, but they take effect only when you apply them to an AAA service.

To configure the LDAP server groups, follow these steps:

	Command	Purpose
Step 1	`switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	`switch(config)# aaa group server ldap LDAPServer1` `switch(config-ldap)#`	Creates an LDAP server group and enters the LDAP server group configuration mode for that group.
Step 3	`switch(config-ldap)# server 10.10.2.2`	Configures the LDAP server as a member of the LDAP server group. If the specified LDAP server is not found, configure it using the ldap-server host command and retry this command.
Step 4	`switch(config-ldap)# authentication compare password-attribute TyuL8r`	(Optional) Performs LDAP authentication using the bind or compare method. The default LDAP authentication method is the bind method using first search and then bind.

	Command	Purpose
Step 5	`switch(config-ldap)# enable user-server-group`	(Optional) Enables group validation. The group name should be configured in the LDAP server. Users can login through public-key authentication only if the username is listed as a member of this configured group in the LDAP server.
Step 6	`switch(config-ldap)# enable Cert-DN-match`	(Optional) Enables users to login only if the user profile lists the subject-DN of the user certificate as authorized for login.
Step 7	`switch(config)# exit` `switch#`	Exits configuration mode.
Step 8	`switch# show ldap-server groups`	(Optional) Displays the LDAP server group configuration.
Step 9	`switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring the Global LDAP Timeout Interval

You can set a global timeout interval that determines how long the Cisco NX-OS device waits for responses from all LDAP servers before declaring a timeout failure.

To configure the global LDAP timeout interval, follow these steps:

Step 1	`switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	`switch(config)# ldap-server timeout 10`	Specifies the timeout interval for LDAP servers. The default timeout interval is 5 seconds. The range is from 1 to 60 seconds.
Step 3	`switch(config)# exit` `switch#`	Exits configuration mode.
Step 4	`switch# show ldap-server`	(Optional) Displays the LDAP server configuration.
Step 5	`switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring the Timeout Interval for an LDAP Server

You can set a timeout interval that determines how long the Cisco NX-OS device waits for responses from an LDAP server before declaring a timeout failure.

To configure the timeout interval for an LDAP server, follow these steps:

Step 1	`switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	`switch(config)# ldap-server host server1 timeout 10`	Specifies the timeout interval for a specific server. The default is the global value. **Note** The timeout interval value specified for an LDAP server overrides the global timeout interval value specified for all LDAP servers.
Step 3	`switch(config)# exit` `switch#`	Exits configuration mode.
Step 4	`switch# show ldap-server`	(Optional) Displays the LDAP server configuration.
Step 5	`switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring the Global LDAP Server Port

You can configure a global LDAP server port through which clients initiate TCP connections. By default, Cisco NX-OS devices use port 389 for all LDAP requests.

To configure the global LDAP server port, follow these steps:

Step 1	`switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	`switch(config)# ldap-server port 2`	Specifies the global TCP port to use for LDAP messages to the server. The default TCP port is 389. The range is from 1 to 65535.
Step 3	`switch(config)# exit` `switch#`	Exits configuration mode.
Step 4	`switch# show ldap-server`	(Optional) Displays the LDAP server configuration.
Step 5	`switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring TCP Ports

You can configure another TCP port for the LDAP servers if there are conflicts with another application. By default, Cisco NX-OS devices use port 389 for all LDAP requests.

To configure the TCP ports, follow these steps:

Step 1	`switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	`switch(config)# ldap-server host 10.10.1.1 port 200 timeout 5`	Specifies the TCP port to use for LDAP messages to the server. The default TCP port is 389. The range is from 1 to 65535. Optionally specifies the timeout interval for the server. The range is from 1 to 60 seconds, and the default timeout is the global value or 5 seconds if a global value is not configured. **Note** The timeout interval value specified for an LDAP server overrides the global timeout interval value specified for all LDAP servers.
Step 3	`switch(config)# exit` `switch#`	Exits configuration mode.
Step 4	`switch# show ldap-server`	(Optional) Displays the LDAP server configuration.
Step 5	`switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring LDAP Search Maps

You can configure LDAP search maps to send a search query to the LDAP server. The server searches its database for data meeting the criteria specified in the search map.

To configure the LDAP search maps, follow these steps:

Step 1	`switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	`switch(config)# ldap search-map map1` `switch(config-ldap-search-map)#`	Configures an LDAP search map.
Step 3	`switch(config-ldap-search-map)# userprofile attribute-name description search-filter (&(objectClass=inetOrgPerson)(cn =$userid)) base-DN dc=acme,dc=com`	(Optional) Configures the attribute name, search filter, and base-DN for the user profile, trusted certificate, CRL, certificate DN match, public key match, or user-switchgroup lookup search operation. These values are used to send a search query to the LDAP server.
Step 4	`switch(config-ldap-search-map)# exit` `switch(config)#`	Exits LDAP search map configuration mode.
Step 5	`switch(config)# show ldap-search-map`	(Optional) Displays the configured LDAP search maps.
Step 6	`switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring the LDAP Dead-Time Interval

You can configure the dead-time interval for all LDAP servers. The dead-time interval specifies the time that the Cisco NX-OS device waits, after declaring that an LDAP server is dead, before sending out a test packet to determine if the server is now alive.

Note When the dead-time interval is 0 minutes, LDAP servers are not marked as dead even if they are not responding. You can configure the dead-time interval per group.

Detailed Steps

To configure the LDAP dead-time interval, follow these steps:

Step 1	`switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	`switch(config)# ldap-server deadtime 5`	Configures the global dead-time interval. The default value is 0 minutes. The range is from 1 to 60 minutes.
Step 3	`switch(config)# exit` `switch#`	Exits configuration mode.
Step 4	`switch#show ldap-server`	(Optional) Displays the LDAP server configuration.
Step 5	`switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring AAA Authorization on LDAP Servers

You can configure the default AAA authorization method for LDAP servers.

To configure the AAA authorization on LDAP servers, follow these steps:

Step 1	`switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	`switch(config)# aaa authorization ssh-certificate default group LDAPServer1 LDAPServer2`	Configures the default AAA authorization method for the LDAP servers. The **ssh-certificate** keyword configures LDAP or local authorization with certificate authentication, and the ssh-publickey keyword configures LDAP or local authorization with the **SSH public key**. The default authorization is local authorization, which is the list of authorized commands for the user's assigned role. The group-list argument consists of a space-delimited list of LDAP server group names. Servers that belong to this group are contacted for AAA authorization. The `local` method uses the local database for authorization.

Step 3	`switch(config)# exit` `switch#`	Exits configuration mode.
Step 4	`switch(config)# show aaa authorization`	(Optional) Displays the AAA authorization configuration. The all keyword displays the default values.
Step 5	`switch(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Disabling LDAP

When you disable LDAP, all related configurations are automatically discarded.

To disable LDAP, follow these steps:

Step 1	`switch# configure terminal` `switch(config)#`	Enters global configuration mode.
Step 2	`switch(config)# no feature ldap`	Disables LDAP.
Step 3	`switch(config)# exit` `switch#`	Exits configuration mode.
Step 4	`switch# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

For detailed information about the fields in the output from this command, see the *Cisco MDS 9000 Family Command Reference, Release 5.0(1a)*.

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.

To specify the host RADIUS server IPv4 address and other options, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius-server host 10.10.0.0 key HostKey`	Specifies the preshared key for the selected RADIUS server. This key overrides the key assigned using the **radius-server key** command. In this example, the host is 10.10.0.0 and the key is HostKey.
Step 3	`switch(config)# radius-server host 10.10.0.0 auth-port 2003`	Specifies the destination UDP port number to which the RADIUS authentication messages should be sent. In this example, the host is 10.10.0.0 and the authentication port is 2003. The default authentication port is 1812, and the valid range is 0 to 65366.

	Command	Purpose
Step 4	`switch(config)# radius-server host 10.10.0.0 acct-port 2004`	Specifies the destination UDP port number to which RADIUS accounting messages should be sent. The default accounting port is 1813, and the valid range is 0 to 65366.
Step 5	`switch(config)# radius-server host 10.10.0.0 accounting`	Specifies this server to be used only for accounting purposes. **Note** If neither the **authentication** nor the **accounting** options are specified, the server is used for both accounting and authentication purposes.
Step 6	`switch(config)# radius-server host 10.10.0.0 key 0 abcd`	Specifies a clear text key for the specified server. The key is restricted to 64 characters.
	`switch(config)# radius-server host 10.10.0.0 key 4 da3Asda2ioyuoiuH`	Specifies an encrypted key for the specified server. The key is restricted to 64 characters.

To specify the host RADIUS server IPv6 address and other options, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius-server host 2001:0DB8:800:200C::417A Key HostKey`	Specifies the preshared key for the selected RADIUS server. This key overrides the key assigned using the **radius-server key** command. In this example, the host is 2001:0DB8:800:200C::417A and the key is HostKey.
Step 3	`switch(config)# radius-server host 2001:0DB8:800:200C::417A auth-port 2003`	Specifies the destination UDP port number to which the RADIUS authentication messages should be sent. In this example, the host is 2001:0DB8:800:200C::417A and the authentication port is 2003. The default authentication port is 1812, and the valid range is 0 to 65366.
Step 4	`switch(config)# radius-server host 2001:0DB8:800:200C::417A acct-port 2004`	Specifies the destination UDP port number to which RADIUS accounting messages should be sent. The default accounting port is 1813, and the valid range is 0 to 65366.
Step 5	`switch(config)# radius-server host 2001:0DB8:800:200C::417A accounting`	Specifies this server to be used only for accounting purposes. **Note** If neither the **authentication** nor the **accounting** options are specified, the server is used for both accounting and authentication purposes.
Step 6	`switch(config)# radius-server host 2001:0DB8:800:200C::417A key 0 abcd`	Specifies a clear text key for the specified server. The key is restricted to 64 characters.
	`switch(config)# radius-server host 2001:0DB8:800:200C::417A key 4 da3Asda2ioyuoiuH`	Specifies an encrypted key for the specified server. The key is restricted to 64 characters.

To specify the host RADIUS server DNS name and other options, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius-server host radius2 key HostKey`	Specifies the preshared key for the selected RADIUS server. This key overrides the key assigned using the **radius-server key** command. In this example, the host is radius2 and the key is HostKey.
Step 3	`switch(config)# radius-server host radius2 auth-port 2003`	Specifies the destination UDP port number to which the RADIUS authentication messages should be sent. In this example, the host is radius2 and the authentication port is 2003. The default authentication port is 1812, and the valid range is 0 to 65366.
Step 4	`switch(config)# radius-server host radius2 acct-port 2004`	Specifies the destination UDP port number to which RADIUS accounting messages should be sent. The default accounting port is 1813, and the valid range is 0 to 65366.
Step 5	`switch(config)# radius-server host radius2 accounting`	Specifies this server to be used only for accounting purposes. **Note** If neither the **authentication** nor the **accounting** options are specified, the server is used for both accounting and authentication purposes.
Step 6	`switch(config)# radius-server host radius2 key 0 abcd`	Specifies a clear text key for the specified server. The key is restricted to 64 characters.
	`switch(config)# radius-server host radius2 key 4 da3Asda2ioyuoiuH`	Specifies an encrypted key for the specified server. The key is restricted to 64 characters.

Configuring the Default RADIUS Server Encryption Type and Preshared Key

To configure the RADIUS preshared key, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius-server key AnyWord`	Configures a preshared key (AnyWord) to authenticate communication between the RADIUS client and server. The default is clear text.
	`switch(config)# radius-server key 0 AnyWord`	Configures a preshared key (AnyWord) specified in clear text (indicated by 0) to authenticate communication between the RADIUS client and server.
	`switch(config)# radius-server key 7 abe4DFeeweo00o`	Configures a preshared key (specified in encrypted text) specified in encrypted text (indicated by 7) to authenticate communication between the RADIUS client and server.

To configure the default RADIUS server encryption type and preshared key, 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.

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 RADIUS Server Timeout Interval

You can configure a global timeout value between transmissions for all RADIUS servers.

Note If timeout values are configured for individual servers, those values override the globally configured values.

To specify the timeout values between retransmissions to the RADIUS servers, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius-server timeout 30`	Configures the global timeout period in seconds for the switch to wait for a response from all TACACS+ servers before the switch declares a timeout failure. The time ranges from 1 to 1440 seconds.
	`switch(config)# no radius-server timeout 30`	Reverts the transmission time to the default value (1 second).

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 specify the number of times that RADIUS servers should try to authenticate a user, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius-server retransmit 3`	Configures the number of times (3) the switch tries to connect to a RADIUS server(s) before reverting to local authentication.
	`switch(config)# no radius-server retransmit`	Reverts to the default retry count (1).

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

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

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 idle timer, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius-server host 10.1.1.1 test idle-time 20`	Configures the test idle time interval value in minutes. The valid range is 1 to 1440 minutes.
Step 3	`switch(config)# no radius-server host 10.1.1.1 test idle-time 20`	Reverts to the default value (0 minutes).

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, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius-server host 10.1.1.1 test username testuser`	Configures the test user (testuser) with the default password (test). The default user name is test.
	`switch(config)# no radius-server host 10.1.1.1 test username testuser`	Removes the test user name (testuser).
	`switch(config)# radius-server host 10.1.1.1 test username testuser password Ur2Gd2BH`	Configures the test user (testuser) and assigns a strong password.

Configuring the Dead Timer

The dead timer specifies the interval that the MDS switch waits, after declaring that a RADIUS server is dead, before sending out a test packet to determine if the server is now alive.

Note The default dead timer value is 0 minutes. When the dead timer interval is 0 minutes, RADIUS server monitoring is not performed unless the RADIUS server is part of a server group and the dead-time interval for the group is greater than 0 minutes. (See the "Server Groups" section on page 29-63).

Note If the dead timer of a dead RADIUS server expires before it is sent a RADIUS test message, that server is marked as alive again even if it is still not responding. To avoid this scenario, configure a test user with a shorter idle time than the dead timer time.

To configure the dead timer, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius-server deadtime 30`	Configures the dead timer interval value in minutes. The valid range is 1 to 1440 minutes.
Step 3	`switch(config)# no radius-server deadtime 30`	Reverts to the default value (0 minutes).

Configuring an LDAP Server

To configure an LDAP server and all of its options, follow these steps:

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

You see the LDAP configuration in the Information pane.

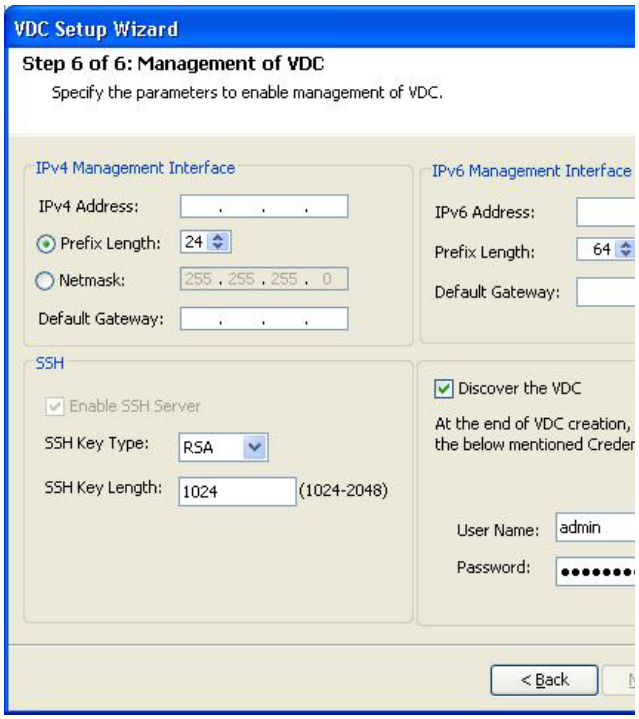
Step 2 Click the **Servers** tab.

You see any existing RADIUS servers.

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

You see the Create LDAP Server dialog box.

Figure 29-3 LDAP Server Creation



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

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

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

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

Step 8 (Optional) Modify the authentication and accounting ports used by this LDAP server.

Step 9 Select the appropriate key type for the LDAP 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 an LDAP 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.

Creating LDAP Search Map

To create an LDAP search map, follow these steps:

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

You see the LDAP configuration in the Information pane.

Step 2 Click the **Search Map** tab.

Step 3 Click **Create Row** to add a new LDAP search map.

Step 4 Enter the LDAP search map name for the **Name** field.

Step 5 Select the appropriate search type for the **Type** field.

Step 6 Enter the base domain name for the **BaseDN** field.

Step 7 Enter the filter value for the **Filter** field.

Step 8 Enter the attribute value for the **Attribute** field.

Step 9 Click **Create** to save the changes.

Configuring a RADIUS Server

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

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

You see the RADIUS configuration in the Information pane.

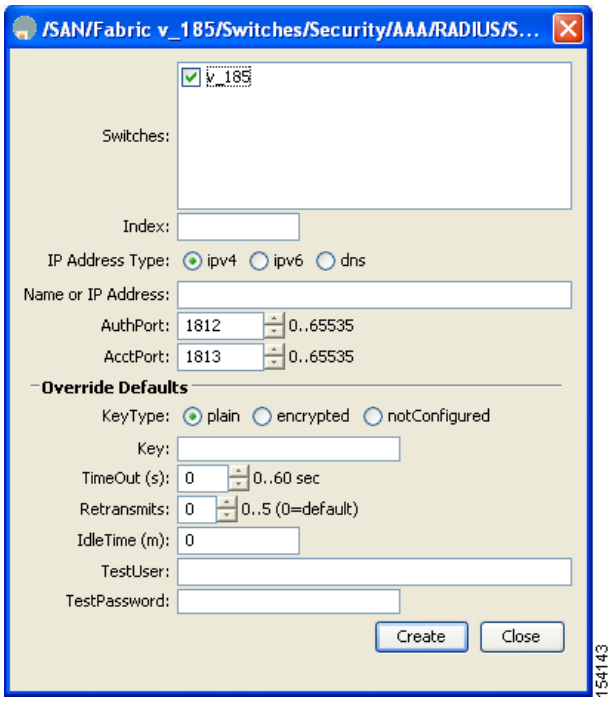
Step 2 Click the **Servers** tab.

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 29-4.

Figure 29-4 Create RADIUS Server



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 (Optional) 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.

Validating a RADIUS Server

To configure the switch to periodically test a RADIUS server, 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 29-4).

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.

Sending RADIUS Test Messages for Monitoring

You can manually send test messages to monitor a RADIUS server.

To send the test message to the RADIUS server, follow this step:

	Command	Purpose
Step 1	`switch# test aaa server radius 10.10.1.1 test test`	Sends a test message to a RADIUS server using the default username (test) and password (test).
	`switch# test aaa server radius 10.10.1.1 testuser Ur2Gd2BH`	Sends a test message to a RADIUS server using a configured test username (testuser) and password (Ur2Gd2BH). **Note** A configured username and password is optional (see the "Configuring Test User Name" section on page 29-93).

Allowing Users to Specify 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.

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

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius-server directed-request`	Allows users to specify a RADIUS server to send the authentication request when logging in.
	`switch(config)# no radius-server directed-request`	Reverts to sending the authentication request to the first server in the server group (default).

To allow users logging into an MDS switch to select a RADIUS server for authentication, 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.

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.

To enable TACACS+ for a Cisco MDS switch, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# feature tacacs+`	Enables the TACACS+ in this switch.
	`switch(config)# no feature tacacs+`	Disables (default) the TACACS+ in this switch.

Setting the Default TACACS+ Server Encryption Type and Preshared Key

To configure the default TACACS+ server encryption type and preshared key, 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 TACACS+ Server Address

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 (see the "Setting the Default TACACS+ Server Timeout Interval and Retransmits" section on page 29-101).

Note You can use the dollar sign ($) and the percent sign (%) in global secret keys.

To configure the TACACS+ server IPv4 address and other options, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# tacacs-server host 171.71.58.91`	Configures the TACACS+ server identified by the specified IPv4 address.
	`switch(config)# no tacacs-server host 171.71.58.91`	Deletes the specified TACACS+ server identified by the IPv4 address. By default, no server is configured.
Step 3	`switch(config)# tacacs-server host 171.71.58.91 port 2`	Configures the TCP port for all TACACS+ requests.
	`switch(config)# no tacacs-server host 171.71.58.91 port 2`	Reverts to the factory default of using port 49 for server access.
Step 4	`switch(config)# tacacs-server host 171.71.58.91 key MyKey`	Configures the TACACS+ server identified by the specified domain name and assigns the secret key.
Step 5	`switch(config)# tacacs-server host 171.71.58.91 timeout 25`	Configures the timeout period for the switch to wait for a response from the specified server before it declares a timeout failure.

To configure the TACACS+ server IPv6 address and other options, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# tacacs-server host 2001:0DB8:800:200C::417A` `warning: no key is configured for the host`	Configures the TACACS+ server identified by the specified IPv6 address.
	`switch(config)# no tacacs-server host 2001:0DB8:800:200C::417A`	Deletes the specified TACACS+ server identified by the IPv6 address. By default, no server is configured.
Step 3	`switch(config)# tacacs-server host 2001:0DB8:800:200C::417A port 2`	Configures the TCP port for all TACACS+ requests.
	`switch(config)# no tacacs-server host 2001:0DB8:800:200C::417A port 2`	Reverts to the factory default of using port 49 for server access.
Step 4	`switch(config)# tacacs-server host 2001:0DB8:800:200C::417A key MyKey`	Configures the TACACS+ server identified by the specified domain name and assigns the secret key.
Step 5	`switch(config)# tacacs-server host 2001:0DB8:800:200C::417A timeout 25`	Configures the timeout period for the switch to wait for a response from the specified server before it declares a timeout failure.

To configure the TACACS+ server DNS name and other options, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# tacacs-server host host1.cisco.com` `warning: no key is configured for the host`	Configures the TACACS+ server identified by the specified DNS name.
	`switch(config)# no tacacs-server host host1.cisco.com`	Deletes the specified TACACS+ server identified by the DNS name. By default, no server is configured.
Step 3	`switch(config)# tacacs-server host host1.cisco.com port 2`	Configures the TCP port for all TACACS+ requests.
	`switch(config)# no tacacs-server host host1.cisco.com port 2`	Reverts to the factory default of using port 49 for server access.
Step 4	`switch(config)# tacacs-server host host1.cisco.com key MyKey`	Configures the TACACS+ server identified by the specified domain name and assigns the secret key.
Step 5	`switch(config)# tacacs-server host host1.cisco.com timeout 25`	Configures the timeout period for the switch to wait for a response from the specified server before it declares a timeout failure.

Setting the Global Secret Key

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.

Note You can use the dollar sign ($) and the percent sign (%) in global secret keys.

To set the secret key for TACACS+ servers, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# tacacs-server key 7 3sdaA3daKUngd`	Assigns the global secret key (in encrypted format) to access the TACACS+ server. This example specifies **7** to indicate the encrypted format being used. If this global key and the individual server keys are not configured, clear text messages are sent to the TACACS+ server(s).
	`switch(config)# no tacacs-server key oldPword`	Deletes the configured global secret key to access the TACACS+ server and reverts to the factory default of allowing access to all configured servers.

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, 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. (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.

Setting the Timeout Value

You can configure a global timeout value between transmissions for all TACACS+ servers.

Note If timeout values are configured for individual servers, those values override the globally configured values.

To set the global timeout value for TACACS+ servers, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# tacacs-server timeout 30`	Configures the global timeout period in seconds for the switch to wait for a response from all TACACS+ servers before the switch declares a timeout failure. The time ranges from 1 to 1440 seconds.
	`switch(config)# no tacacs-server timeout 30`	Deletes the configured timeout period and reverts to the factory default of 5 seconds.

Configuring a TACACS+ Server

To configure a TACACS+ server and all its options using DCNM-SAN, follow these steps:

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

You see the TACACS+ configuration in the Information pane.

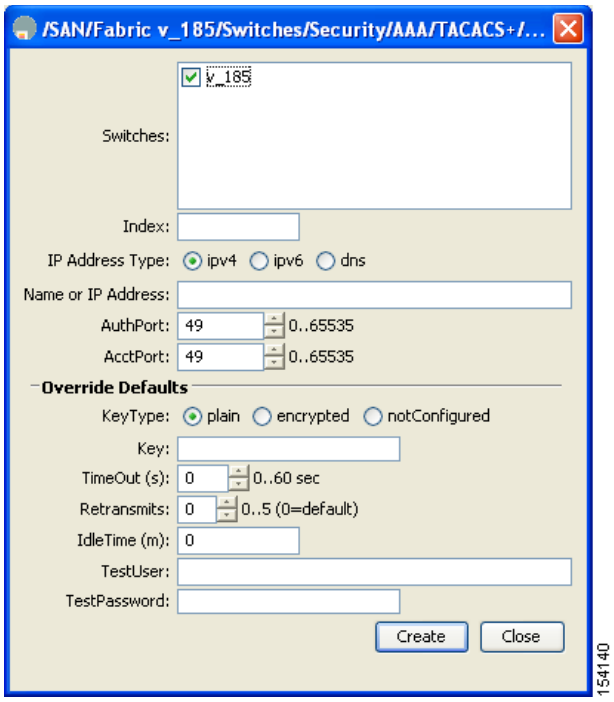
Step 2 Click the **Servers** tab.

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 29-5.

Figure 29-5 Create TACACS+ Server Dialog Box



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.

Configuring the TACACS+ Test Idle Timer

The test idle timer specifies the interval during which a TACACS+ 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 TACACS+ server monitoring is not performed.

To configure the idle timer, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# tacacs-server host 10.1.1.1 test idle-time 20`	Configures the test idle time interval value in minutes. The valid range is 1 to 1440 minutes.
Step 3	`switch(config)# no tacacs-server host 10.1.1.1 test idle-time 20`	Reverts to the default value (0 minutes).

Configuring Test Username

You can configure a username and password for periodic TACACS+ server status testing. You do not need to configure the user name and password to monitor TACACS+ servers. You can use the default test username (test) and default password (test).

To configure the optional username and password for periodic TACACS+ server status testing, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# tacacs-server host 10.1.1.1 test username testuser`	Configures the test user (testuser) with the default password (test). The default username is test.
	`switch(config)# no tacacs-server host 10.1.1.1 test username testuser`	Removes the test user (testuser).
	`switch(config)# tacacs-server host 10.1.1.1 test username testuser password Ur2Gd2BH`	Configures the test user (testuser) and assigns a strong password. For guidelines for creating strong passwords, see the "Characteristics of Strong Passwords" section on page 28-30.

Configuring the Dead Timer

The dead timer specifies the interval that the MDS switch waits, after declaring a TACACS+ server is dead, before sending out a test packet to determine if the server is now alive.

Note The default dead timer value is 0 minutes. TACACS+ server monitoring is not performed if the dead timer interval is 0 minutes, unless the TACACS+ server is a part of a bigger group with the dead-time interval greater than 0 minutes. (See "Configuring the RADIUS, TACACS+, and LDAP Server" section on page 29-78).

Note If the dead timer of a dead TACACS+ server expires before it is sent a TACACS+ test message, that server is marked as alive again even if it is still not responding. To avoid this scenario, configure a test user with a shorter idle time than the dead timer time.

To configure the dead timer, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# tacacs-server deadtime 30`	Configures the dead-time interval value in minutes. The valid range is 1 to 1440 minutes.
	`switch(config)# no tacacs-server deadtime 30`	Reverts to the default value (0 minutes). **Note** When the dead-time interval is 0 minutes, TACACS+ server monitoring is not performed unless the TACACS+ server is part of a server group and the dead-time interval for the group is greater than 0 minutes. (See the "Configuring the RADIUS, TACACS+, and LDAP Server" section on page 29-78).

Sending TACACS+ Test Messages for Monitoring

You can manually send test messages to monitor a TACACS+ server.

To send the test message to the TACACS+ server, follow these steps:

Command	Purpose
`switch# test aaa server tacacs+ 10.10.1.1 test test`	Sends a test message to a TACACS+ server using the default username (test) and password (test).
`switch# test aaa server tacacs+ 10.10.1.1 testuser Ur2Gd2BH`	Sends a test message to a TACACS+ server using a configured test username and password. A configured username and password is optional (see the "Configuring Test Username" section on page 29-104).

Allowing Users to Specify a TACACS+ Server at Login

To allow users logging into an MDS switch to select a TACACS+ server for authentication, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# tacacs-server directed-request`	Allows users to specify a TACACS+ server to send the authentication request when logging in.
	`switch(config)# no tacacs-server directed-request`	Reverts to sending the authentication request to the first server in the server group (default).

To configure the switch to allow users to specify a TACACS+ server at login using DCNM-SAN, 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.

Clearing TACACS+ Server Statistics

You can clear all the TACACS+ server statistics using the **clear tacacs-server statistics 10.1.2.3** command.

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.

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 29-64).

Restrictions

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 DCNM-SAN or Device Manager users.

Note Configuration of a TACACS+ group fails if MSCHPv2 authentication is not disabled.

To configure a RADIUS server group, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# aaa group server radius RadServer` `switch(config-radius)#`	Creates a server group named RadServer and enters the RADIUS server group configuration submode for that group.
	`switch(config)# no aaa group server radius RadServer`	Deletes the server group called RadServer from the authentication list.
Step 3	`switch(config-radius)# server 10.71.58.91`	Configures the RADIUS server at IPv4 address 10.71.58.91 to be tried first within the server group RadServer. **Tip** If the specified RADIUS server is not found, configure it using the **radius-server host** command and retry this command.

	Command	Purpose
Step 4	`switch(config-radius)# server 2001:0DB8:800:200C::417A`	Configures the RADIUS server at IPv6 address 2001:0DB8:800:200C::417A to be tried first within the server group RadServer.
	`switch(config-radius)# no server 2001:0DB8:800:200C::417A`	Removes the RADIUS server at IPv6 address 2001:0DB8:800:200C::417A from the server group RadServer.
Step 5	`switch(config-radius)# exit`	Returns to configuration mode.
Step 6	`switch(config)# aaa group server radius RadiusServer` `switch(config-radius)#`	Creates a server group named RadiusServer and enters the RADIUS server group configuration submode for that group.
Step 7	`switch(config-radius)# server ServerA`	Configures ServerA to be tried first within the server group called the RadiusServer1. **Tip** If the specified RADIUS server is not found, configure it using the **radius-server host** command and retry this command.
Step 8	`switch(config-radius)# server ServerB`	Configures ServerB to be tried second within the server group RadiusServer1.
Step 9	`switch(config-radius)# deadtime 30`	Configures the monitoring dead time to 30 minutes. The range is 0 through 1440. **Note** If the dead-time interval for an individual RADIUS server is greater than 0, that value takes precedence over the value set for the server group.
	`switch(config-radius)# no deadtime 30`	Reverts to the default value (0 minutes). **Note** If the dead-time interval for both the RADIUS server group and an individual TACACS+ server in the RADIUS server group is set to 0, the switch does not mark the RADIUS server as dead when it is found to be unresponsive by periodic monitoring. Also, the switch does not perform dead server monitoring for that RADIUS server. (See the "Configuring the RADIUS, TACACS+, and LDAP Server" section on page 29-78).

To configure a TACACS+ server group, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# aaa group server tacacs+ TacacsServer1` `switch(config-tacacs+)#`	Creates a server group named TacacsServer1 and enters the submode for that group.
	`switch(config)# no aaa group server tacacs+ TacacsServer1`	Deletes the server group called TacacsServer1 from the authentication list.

	Command	Purpose
Step 3	`switch(config-tacacs+)# server ServerA`	Configures ServerA to be tried first within the server group called the TacacsServer1. **Tip** If the specified TACACS+ server is not found, configure it using the **tacacs-server host** command and retry this command.
Step 4	`switch(config-tacacs+)# server ServerB`	Configures ServerB to be tried second within the server group TacacsServer1.
	`switch(config-tacacs+)# no server ServerB`	Deletes ServerB within the TacacsServer1 list of servers.
Step 5	`switch(config-tacacs+)# deadtime 30`	Configures the monitoring dead time to 30 minutes. The range is 0 through 1440. **Note** If the dead-time interval for an individual TACACS+ server is greater than 0, that value takes precedence over the value set for the server group.
	`switch(config-tacacs+)# no deadtime 30`	Reverts to the default value (0 minutes). **Note** If the dead-time interval for both the TACACS+ server group and an individual TACACS+ server in the TACACS+ server group is set to 0, the switch does not mark the TACACS+ server as dead when it is found to be unresponsive by periodic monitoring. Also, the switch does not perform dead server monitoring for that TACACS+ server. (See the "Configuring a TACACS+ Server" section on page 29-102).

To configure a RADIUS, TACACS+, or LDAP server group using DCNM-SAN, follow these steps:

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

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

You see the RADIUS, TACACS+, or LDAP server groups configured.

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

You see the Create Server dialog box.

Step 3 Click the **radius** radio button to add a RADIUS server group, the **tacacs+** radio button to add a TACACS+ server group, and the **ldap** radio button to add a LDAP server group.

Step 4 Supply server names for the ServerIdList field.

Step 5 When you chose LDAP, enter the LDAP search map name for the LDAPSearchMapName.

- LDAPSSLMODE—Specifies if the TLS tunnel should be setup before binding with the LDAP server.
- LDAPBindFirst—Specifies if the user bind should be completed before the search.

Step 6 Click the **plain** radio button to select the plain authentication method, click the **kerberos** button to select the kerberos authentication method, and click **md5digest** to select the md5digest authentication method.

Step 7 Enter the password for the **LDAPComparePasswd** field:

- LDAPCertDNBind—Specifies if the User Certification Bind needs to be checked while doing PKI SSH certificate authorization.
- LDAPUserServerBind—Specifies if the User Server Bind should be checked as part of SSH PKI authorization.

Step 8 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 29-73.

Step 9 Click **Create** to create this server group.

The LDAP Server Group displays LDAP-specific parameters.

Step 10 Click the **Applications** tab to assign this server group to an application.

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

Step 11 Click the **General** tab to assign the type of authentication to this server group.

Check either the MSCHAP or MSCHAPv2 check box based on the type of server group.

Step 12 Click the **Apply Changes** icon to save the changes.

Once the LDAP Server group is created, the configuration information is displayed in two tabs:

- Server Groups—Displays common data shared by all AAA protocols (RADIUS, TACACS+, and LDAP).
- LDAP Server Group—Displays only LDAP-specific protocols.

Enabling AAA Server Distribution

Restrictions

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

To enable RADIUS server distribution, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius distribute`	Enables RADIUS configuration distribution in this switch.
	`switch(config)# no radius distribute`	Disables RADIUS configuration distribution in this switch (default).

To enable TACACS+ server distribution, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# tacacs+ distribute`	Enables TACACS+ configuration distribution in this switch.
	`switch(config)# no tacacs+ distribute`	Disables TACACS+ configuration distribution in this switch (default).

To enable RADIUS server distribution, 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, 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 **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.

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 commit RADIUS configuration changes, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius commit`	Commits the RADIUS configuration changes to the running configuration.

To commit TACACS+ configuration changes, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# tacacs+ commit`	Commits the TACACS+ configuration changes to the running configuration.

To distribute a RADIUS or TACACS+ configuration, 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 Click 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 the RADIUS sessionin-progress distribution, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# radius abort`	Discards the RADIUS configuration changes to the running configuration.

To discard the TACACS+ sessionin-progress distribution, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# tacacs+ abort`	Discards the TACACS+ configuration changes to the running configuration.

To discard RADIUS or TACACS+ distribution, 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 the ongoing CFS distribution session (if any) and to unlock the fabric for the RADIUS feature, enter the **clear radius session** command from any switch in the fabric.

```
switch# clear radius session
```

To clear the ongoing CFS distribution session (if any) and to unlock the fabric for the TACACS+ feature, enter the **clear tacacs+ session** command from any switch in the fabric.

```
switch# clear tacacs+ session
```

To clear a RADIUS or TACACS+ distribution, 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**.

Enabling CHAP Authentication

To enable CHAP authentication, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# aaa authentication login chap enable`	Enables CHAP login authentication.
	`switch# no aaa authentication login chap enable`	Disables CHAP login authentication.

Enabling MSCHAP Authentication

To enable MSCHAP authentication, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# aaa authentication login mschap enable`	Enables MSCHAP login authentication.
Step 3	`switch# no aaa authentication login mschap enable`	Disables MSCHAP login authentication.

To enable MSCHAPv2 authentication, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.

	Command	Purpose
Step 2	`switch(config)# aaa authentication login mschapv2 enable`	Enables MSCHAPv2 login authentication.
Step 3	`switch# no aaa authentication login mschapv2 enable`	Disables MSCHAPv2 login authentication.

Note Password aging, MSCHAPv2, and MSCHAP authentication can fail if one of these authentication is not disabled.

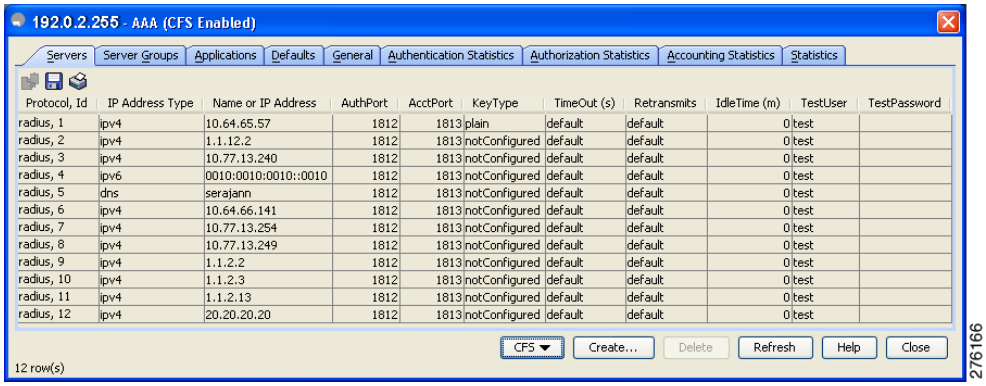
Note A warning message is issued when you execute a command to enable MSCHAPv2 authentication on the TACACS+ server, and the configuration fails.

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

Step 1 Click **Security > AAA.**

You see the AAA configuration in the Information pane (see Figure 29-6).

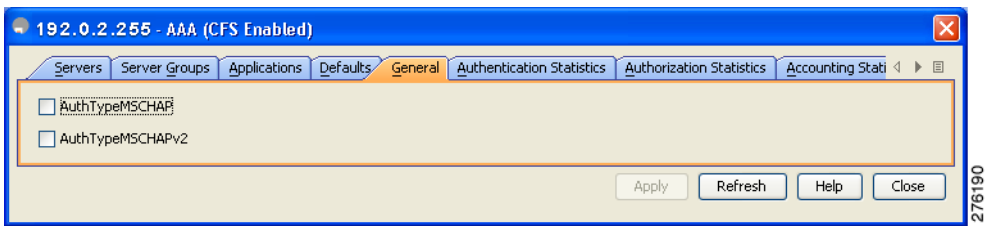
Figure 29-6 AAA Configuration in Device Manager



Step 2 Click the **General** tab.

You see the MSCHAP configuration (see Figure 29-7).

Figure 29-7 MSCHAP Configuration



Step 3 Check the **AuthTypeMSCHAP** or **AuthTypeMSCHAPv2** check box to use MSCHAP or MSCHAPv2 to authenticate users on the switch.

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

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 29-8, Figure 29-9, Figure 29-10, and Figure 29-11 display ACS server user setup configurations for network-admin roles and multiple roles using either RADIUS or TACACS+.

Figure 29-8 Configuring the network-admin Role When Using RADIUS

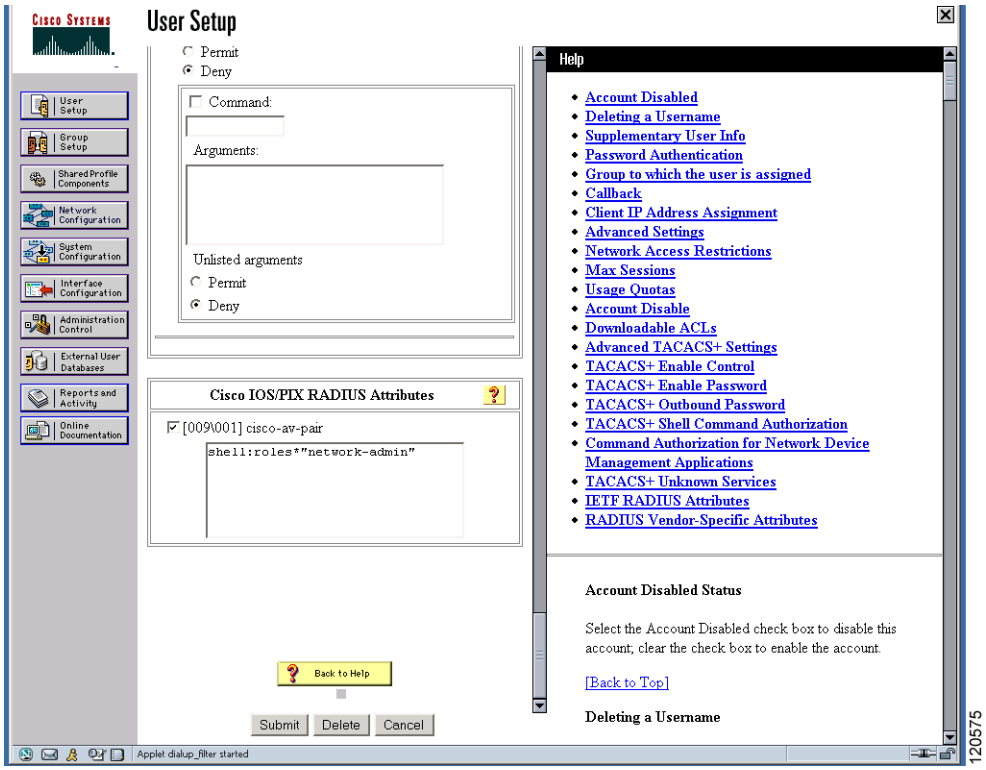


Figure 29-9 Configuring Multiple Roles with SNMPv3 Attributes When Using RADIUS

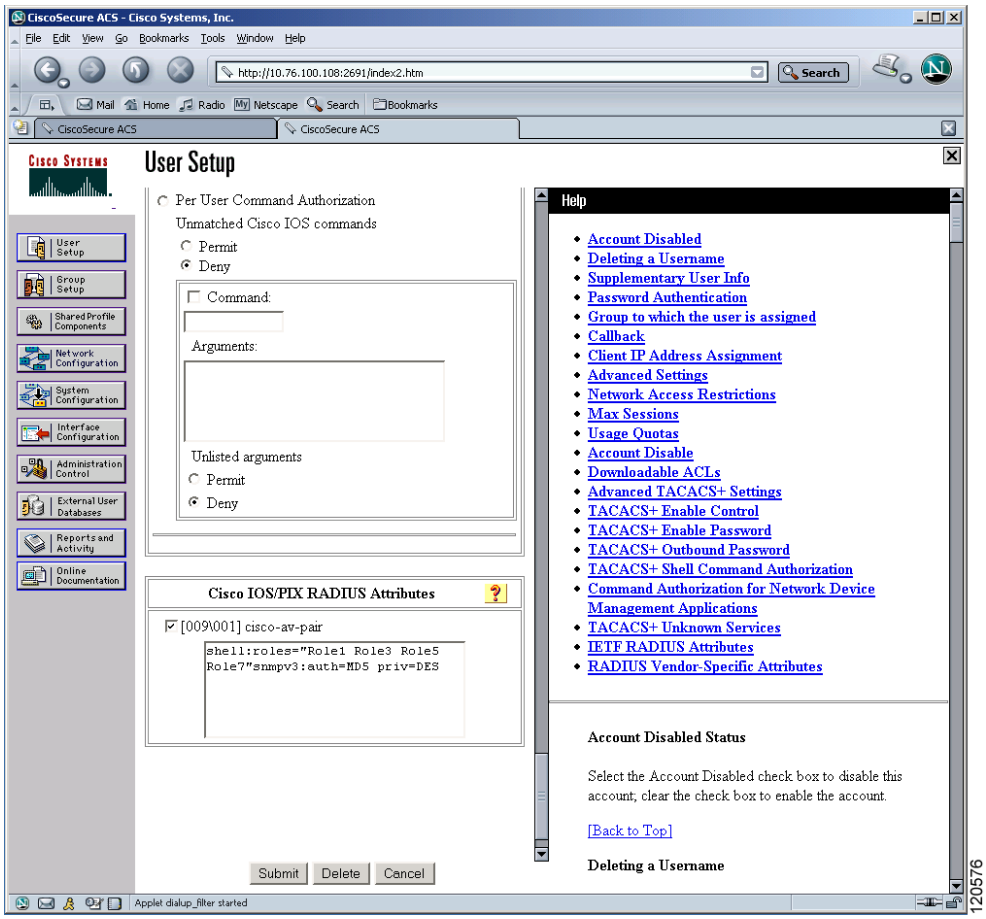


Figure 29-10 Configuring the network-admin Role with SNMPv3 Attributes When Using TACACS+

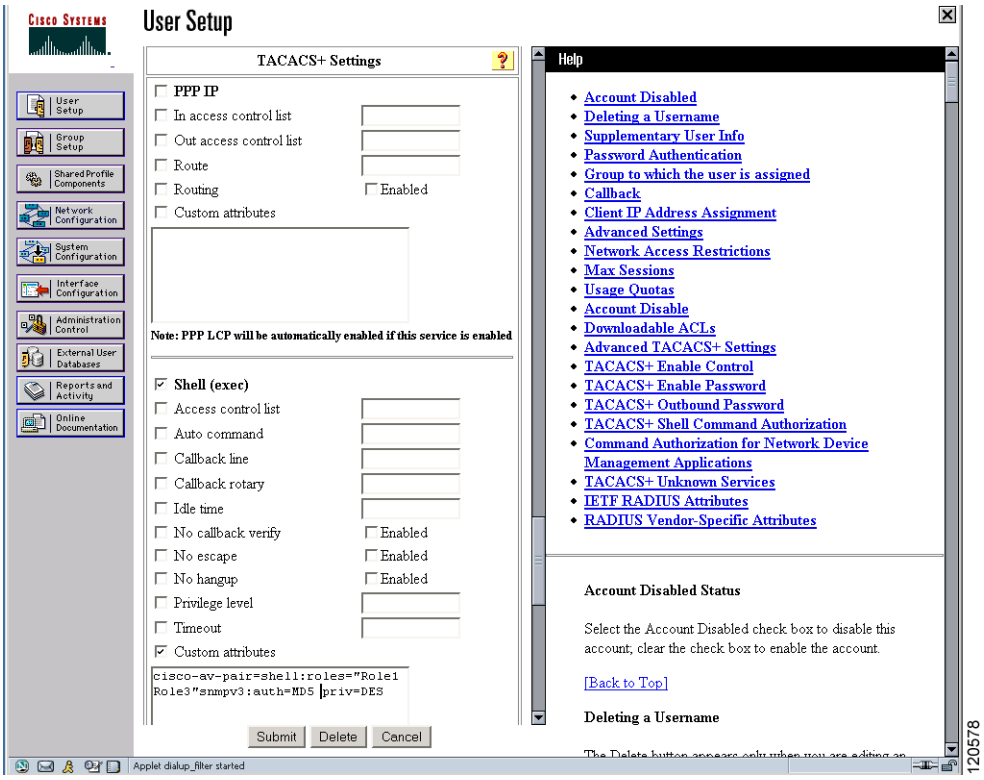
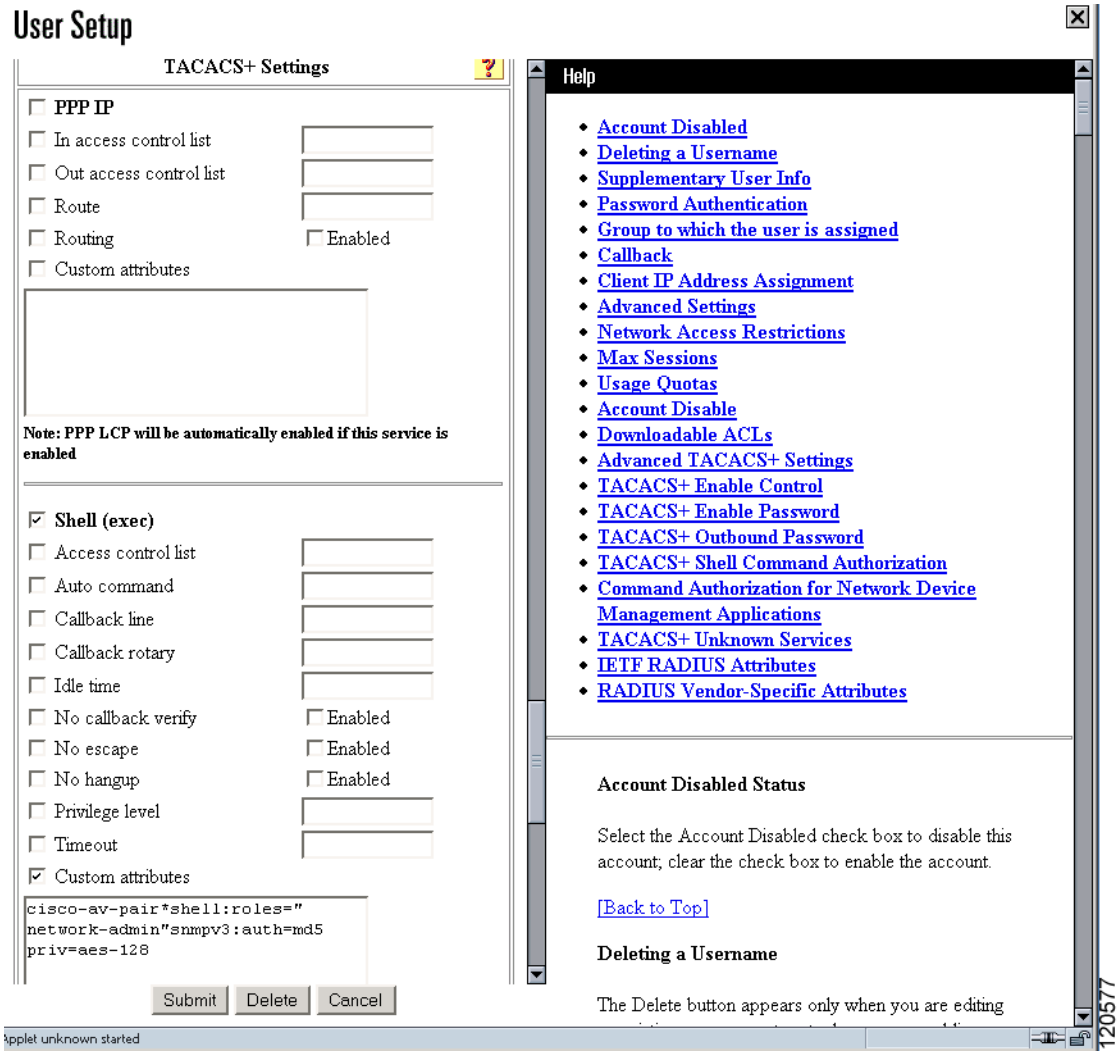


Figure 29-11 Configuring Multiple Roles with SNMPv3 Attributes When Using TACACS+



Verifying RADIUS and TACACS+ Configuration

To display the RADIUS and TACACS+ configuration information, perform one of the following tasks:

Command	Purpose
show show aaa authorization all	Displays aaa Authorization Information Details.
show aaa user default-role	Displays Default User Role for Remote Authentication
show radius-server directed-request	Display the RADIUS directed request configuration.
show tacacs-server directed-request	Display the TACACS+ directed request configuration.

Command	Purpose
show radius-server groups	Verify the configured server group order.
show aaa authentication login chap	Display the CHAP authentication configuration.
show aaa authentication login mschap	Display the MSCHAP authentication configuration.
show aaa authentication login mschapv2	Display the MSCHAPv2 authentication configuration.
show radius-server	Displays Configured RADIUS Information.
show radius-server groups	Displays Configured RADIUS Server-Group Order.
show radius-server statistics 10.1.3.2	Displays RADIUS Server Statistics.
show tacacs-server	Displays Configured TACACS+ Server Information.
show aaa authentication	Displays AAA Authentication Information.
show aaa authentication login error-enable	Displays AAA Authentication Login Information.
show tacacs-server groups	Displays Configured TACACS+ Server Groups.
show aaa groups	Displays All AAA Server Groups.
show tacacs-server statistics 10.1.2.3	Displays TACACS+ Server Statistics.
show radius distribution status	Displays the distribution status on the CFS tab.
show tacacs+ distribution status	Displays the session status once the implicit distribution session has started.
show radius pending-diff	Displays the RADIUS or TACACS+ global and/or server configuration stored in the temporary buffer.
show tacacs+ pending-diff	Displays the TACACS+ global and/or server configuration stored in the temporary buffer.
show radius distribution status	Displays the RADIUS Fabric Merge Status.
show tacacs+ distribution status	Displays the TACACS+ Fabric Merge Status.
show accounting log	Displays the Accounting Log Information.
show aaa authentication	Displays Authentication Information.
show accounting config	Displays Two Samples of Configured Accounting Parameters.
show accounting log 60000	Displays 60,000 Bytes of the Accounting Log.
show accounting log	Displays the Entire Log File.

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

- Displaying RADIUS Server Statistics section, page 29-119
- Displaying RADIUS Server Details section, page 29-119
- Displaying RADIUS Server Statistics section, page 29-120
- Displaying TACACS+ Server Statistics section, page 29-120

Displaying RADIUS Server Statistics

To display RADIUS server statistics, 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.

Displaying RADIUS Server Details

Use the **show radius-server** command to display configured RADIUS parameters as shown in Example 29-2.

Example 29-2 Displays Configured RADIUS Information

```
switch# show radius-server
Global RADIUS shared secret:*******
retransmission count:5
timeout value:10
following RADIUS servers are configured:
        myradius.cisco.users.com:
                available for authentication on port:1812
                available for accounting on port:1813
        172.22.91.37:
                available for authentication on port:1812
                available for accounting on port:1813
                RADIUS shared secret:******
        10.10.0.0:
                available for authentication on port:1812
                available for accounting on port:1813
                RADIUS shared secret:******
```

Example 29-3 Displays Configured RADIUS Server-Group Order

```
switch# show radius-server groups
total number of groups:4
following RADIUS server groups are configured:
        group radius:
                server: all configured radius servers
        group Group1:
                server: Server3 on auth-port 1812, acct-port 1813
                server: Server5 on auth-port 1812, acct-port 1813
```

```
        group Group5:
```

Displaying RADIUS Server Statistics

You can display RADIUS server statistics using the **show radius-server statistics** command.

Example 29-4 Displays RADIUS Server Statistics

```
switch# show radius-server statistics 10.1.3.2
Server is not monitored

Authentication Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0

Accounting Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors:
```

You can clear RADIUS server statistics using the **clear radius-server statistics 10.1.3.2** command.

Displaying TACACS+ Server Statistics

To display TACACS+ server statistics, 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.

Displaying TACACS+ Server Details

Use the **show aaa** and **show tacacs-server** commands to display information about TACACS+ server configuration in all switches in the Cisco MDS 9000 Family as shown in Examples 29-5 to 29-10.

Example 29-5 Displays Configured TACACS+ Server Information

```
switch# show tacacs-server
```

```
Global TACACS+ shared secret:***********
timeout value:30
total number of servers:3

following TACACS+ servers are configured:
        171.71.58.91:
                available on port:2
        cisco.com:
                available on port:49
        171.71.22.95:
                available on port:49
                TACACS+ shared secret:*****
```

Example 29-6 Displays AAA Authentication Information

```
switch# show aaa authentication
         default: group TacServer local none
         console: local
         iscsi: local
         dhchap: local
```

Example 29-7 Displays AAA Authentication Login Information

```
switch# show aaa authentication login error-enable
enabled
```

Example 29-8 Displays Configured TACACS+ Server Groups

```
switch# show tacacs-server groups
total number of groups:2

following TACACS+ server groups are configured:
        group TacServer:
                server 171.71.58.91 on port 2
        group TacacsServer1:
                server ServerA on port 49
                server ServerB on port 49:
```

Example 29-9 Displays All AAA Server Groups

```
switch# show aaa groups
radius
TacServer
```

Example 29-10 Displays TACACS+ Server Statistics

```
switch# show tacacs-server statistics 10.1.2.3
Server is not monitored

Authentication Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0

Authorization Statistics
        failed transactions: 0
        sucessfull transactions: 0
```

```
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0

Accounting Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0
```

Displaying the Session Status

Once the implicit distribution session has started, you can check the session status from DCNM-SAN by expanding **Switches > Security > AAA,** and selecting **RADIUS** or **TACACS+.**

Use the **show radius** command to see the distribution status on the CFS tab.

```
switch# show radius distribution status
distribution : enabled
session ongoing: yes
session owner: admin
session db: exists
merge protocol status: merge activation done


last operation: enable
last operation status: success
```

Once the implicit distribution session has started, you can check the session status using the **show tacacs+ distribution status** command.

```
switch# show tacacs+ distribution status
distribution : enabled
session ongoing: yes
session owner: admin
session db: exists
merge protocol status: merge activation done


last operation: enable
last operation status: success
```

Displaying the Pending Configuration to be Distributed

To display the RADIUS or TACACS+ global and/or server configuration stored in the temporary buffer use the **show radius pending** command, follow these steps:

```
switch(config)# show radius pending-diff
   +radius-server host testhost1 authentication accounting
   +radius-server host testhost2 authentication accounting
```

To display the TACACS+ global and/or server configuration stored in the temporary buffer, use the **show tacacs+ pending** command.

```
switch(config)# show tacacs+ pending-diff
   +tacacs-server host testhost3
   +tacacs-server host testhost4
```

To display the RADIUS or TACACS+ global and/or server configuration stored in the temporary buffer, 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.

Use the **show radius distribution status** command to view the status of the RADIUS fabric merge as shown in Example 29-11.

Example 29-11 Displays the RADIUS Fabric Merge Status

```
switch# show radius distribution status
distribution : enabled
session ongoing: no
session db: does not exist
merge protocol status: merge response received
merge error: conflict: server dmtest2 has auth-port 1812 on this switch and 1999
on remote

last operation: enable
last operation status: success
```

Use the **show tacacs+ distribution status** command to view the status of the TACACS+ fabric merge as shown in Example 29-12.

Example 29-12 Displays the TACACS+ Fabric Merge Status

```
switch# show tacacs+ distribution status
distribution : enabled
session ongoing: no
session db: does not exist
merge protocol status: merge activation done

last operation: enable
last operation status: success
```

Use the **username** command to configure local users and their roles.

Use the **show accounting log** command to view the local accounting log as shown in Example 29-13.

Example 29-13 Displays the Accounting Log Information

```
switch# show accounting log

Thu Dec 10 06:19:21 2009:type=update:id=console0:user=root:cmd=enabled telnet
Thu Dec 10 06:19:21 2009:type=update:id=console0:user=root:cmd=configure termina
```

```
l ; feature telnet (SUCCESS)
Thu Dec 10 06:19:35 2009:type=start:id=171.69.16.56@pts/1:user=admin:cmd=
Thu Dec 10 06:20:16 2009:type=stop:id=171.69.16.56@pts/1:user=admin:cmd=shell te
rminated gracefully
Thu Dec 10 06:20:20 2009:type=stop:id=console0:user=root:cmd=shell terminated gr
acefully
Thu Dec 10 06:29:37 2009:type=start:id=72.163.177.168@pts/1:user=admin:cmd=
Thu Dec 10 06:29:42 2009:type=update:id=72.163.177.168@pts/1:user=admin:cmd=pwd
(SUCCESS)
Thu Dec 10 06:32:49 2009:type=start:id=72.163.190.8@pts/2:user=admin:cmd=
```

Displaying AAA Authentication

The **show aaa authentication** command displays the configured authentication methods as shown in Example 29-14.

Example 29-14 Displays Authentication Information

```
switch# show aaa authentication

    No AAA Authentication
    default: group TacServer local none
    console: local none
    iscsi: local
    dhchap: local
```

Displaying Accounting Configuration

To display configured accounting information use **show accounting** command. See Examples 29-15 to 29-17. To specify the size of the local accounting log to be displayed, use the **show accounting log** command. By default approximately 250 KB of the accounting log is displayed.

Example 29-15 Displays Two Samples of Configured Accounting Parameters

```
switch# show accounting config
show aaa accounting
                default: local

switch# show aaa accounting
                default: group rad1
```

Example 29-16 Displays 60,000 Bytes of the Accounting Log

```
switch# show accounting log 60000
Fri Jan 16 15:28:21 1981:stop:snmp_348506901_64.104.131.208:admin:
Fri Jan 16 21:17:04 1981:start:/dev/pts/0_348527824:admin:
Fri Jan 16 21:35:45 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
Fri Jan 16 21:35:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
Fri Jan 16 21:35:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group5
Fri Jan 16 21:35:55 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group5
```

```
Fri Jan 16 21:35:55 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group3
Fri Jan 16 21:58:17 1981:start:snmp_348530297_171.71.150.105:admin:
...
```

Example 29-17 Displays the Entire Log File

```
switch# show accounting log
Fri Jan 16 15:28:21 1981:stop:snmp_348506901_64.104.131.208:admin:
Fri Jan 16 21:17:04 1981:start:/dev/pts/0_348527824:admin:
Fri Jan 16 21:35:45 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
Fri Jan 16 21:35:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
Fri Jan 16 21:35:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group5
Fri Jan 16 21:35:55 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group5
Fri Jan 16 21:35:55 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group3
Fri Jan 16 21:58:17 1981:start:snmp_348530297_171.71.150.105:admin:
Fri Jan 16 21:58:17 1981:stop:snmp_348530297_171.71.150.105:admin:
Fri Jan 16 21:58:18 1981:start:snmp_348530298_171.71.150.105:admin:
Fri Jan 16 21:58:18 1981:stop:snmp_348530298_171.71.150.105:admin:
...
Fri Jan 16 23:37:02 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group3
Fri Jan 16 23:37:26 1981:update:/dev/pts/0_348527824:admin:updated TACACS+ parameters for
group:TacacsServer1
Fri Jan 16 23:45:19 1981:update:/dev/pts/0_348527824:admin:updated TACACS+ parameters for
group:TacacsServer1
Fri Jan 16 23:45:19 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
...
Fri Jan 16 23:53:51 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
server:Server3
Fri Jan 16 23:54:00 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
server:Server5
Fri Jan 16 23:54:22 1981:update:/dev/pts/0_348527824:admin:updated TACACS+ parameters for
server:ServerA
Fri Jan 16 23:54:25 1981:update:/dev/pts/0_348527824:admin:updated TACACS+ parameters for
server:ServerB
Fri Jan 16 23:55:03 1981:update:/dev/pts/0_348527824:admin:updated RADIUS parameters for
group:Group1
...
Sat Jan 17 00:01:41 1981:start:snmp_348537701_171.71.58.100:admin:
Sat Jan 17 00:01:41 1981:stop:snmp_348537701_171.71.58.100:admin:
Sat Jan 17 00:01:42 1981:start:snmp_348537702_171.71.58.100:admin:
Sat Jan 17 00:01:42 1981:stop:snmp_348537702_171.71.58.100:admin:
...
```

Monitoring RADIUS and TACACS+

This section includes the following topics:

Verifying Authorization Profile

You can verify the authorizaion profile for different commands. When enabled, all commands are directed to the Access Control Server (ACS) for verification. The verification details are displayed once the verification is completed.

```
switch# terminal verify-only username Moheed
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# feature telnet
% Success
switch(config)# feature ssh
% Success
switch(config)# end
% Success
switch# exit
```

Note This command only verifies the commands and does not enable the configuration.

Testing Authorization

You can test the authorization settings for any command.

To test the authorization of a command, use the **test aaa authorization command-type** command.

```
switch(config)# test aaa authorization command-type commands user u1 command "feature
dhcp"
% Success
```

Configuration Examples for LDAP

The following example shows how to configure an LDAP server host and server group:

```
feature ldap
ldap-server host 10.10.2.2 enable-ssl
aaa group server ldap LdapServer
    server 10.10.2.2
exit
show ldap-server
show ldap-server groups
```

The following example shows how to configure an LDAP search map:

```
ldap search-map s0
userprofile attribute-name description search-filter
(&(objectClass=inetOrgPerson)(cn=$userid)) base-DN dc=acme,dc=com
exit
show ldap-search-map
```

The following example shows how to configure AAA authorization with certificate authentication for an LDAP server:

```
aaa authorization ssh-certificate default group LDAPServer1 LDAPServer2
exit
show aaa authorization
```

Feature History for RADIUS, TACACS+, and LDAP

Table 29-6 lists the release history for this feature. Only features that were introduced or modified in Cisco NX-OS Release 5.x or a later release appear in the table.

Table 29-6 Feature History for RADIUS, TACACS+, and LDAP

Feature Name	Releases	Feature Information
Configuring LDAP	5.2	Added LDAP server and server groups configuration.
Switch AAA Functionalities	5.0(1a)	Added configuring fallback mechanism for authentication, configuring AAA server monitoring parameters globally.
Configuring TACACS+ Server Monitoring Parameters	5.0(1a)	Added CHAP authentication.
OTP Authentication	5.0(1a)	Added one-time password support
Merge Guidelines for RADIUS and TACACS+ Configurations	5.0(1a)	TACACS test parameters have to be distributed via CFS; a note has been changed.
AAA Service Configuration Options	5.0(1a)	Note has been changed.