CHAPTER 14

Configuring System Security and AAA Services

Security can be independently configured for each of the following management paths:

- Command-line interface (CLI)—You can access the CLI using one of three connection options:
  - Console (serial connection)
  - Telnet
  - Secure Shell Protocol (SSH)
- Simple Network Management Protocol (SNMP)—The SNMP agent supports security features FOR versions 1, 2c, and 3. Normal SNMP security mechanisms apply to all applications that use SNMP (for example, Cisco MDS 9000 Fabric Manager).

Note Refer to the *Cisco MDS 9000 Family Fabric Manager User Guide* for information on this management tool.

This chapter includes the following sections:

Management Security Features

Table 14-1 shows the security features of the Cisco MDS 9000 Family switches.

Table 14-1 Management Security Features

Security Features	CLI (Console or Telnet/SSH Access)	SNMP (v1, v2c, and v3 access)
User authentication	Local and RADIUS	Local only
Role-based authorization	Local and RADIUS	Local only
Accounting	Local and RADIUS	Local and RADIUS (only logs configuration commands)
Encryption management access	SSH only (not applicable for console or Telnet access)	SNMPv3
Anti-replay attack and prevention of man-in-middle attack		

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

User Authentication

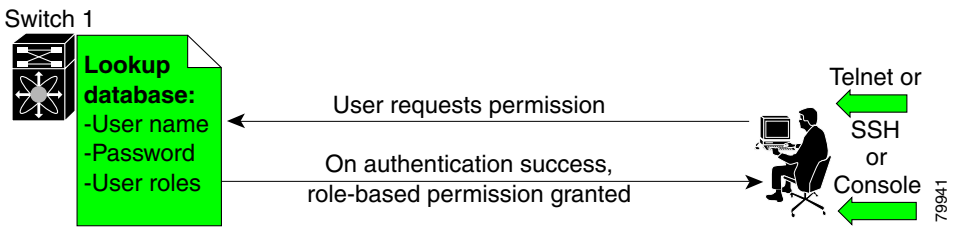
Authentication is the process of verifying the identity of the person managing the switch. This identity verification is based on the user ID and password combination provided by the person trying to manage the switch. Cisco MDS 9000 Family switches allow you to perform local authentication (using the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

For each management path (console or Telnet and SSH), you can enable only one of three options—local, RADIUS, or none. The option can be different for each path.

Local Authentication

The system maintains the user name and password locally and stores the password information in encrypted form. You are authenticated based on the locally stored information (see Figure 14-1).

Figure 14-1 Local Authentication

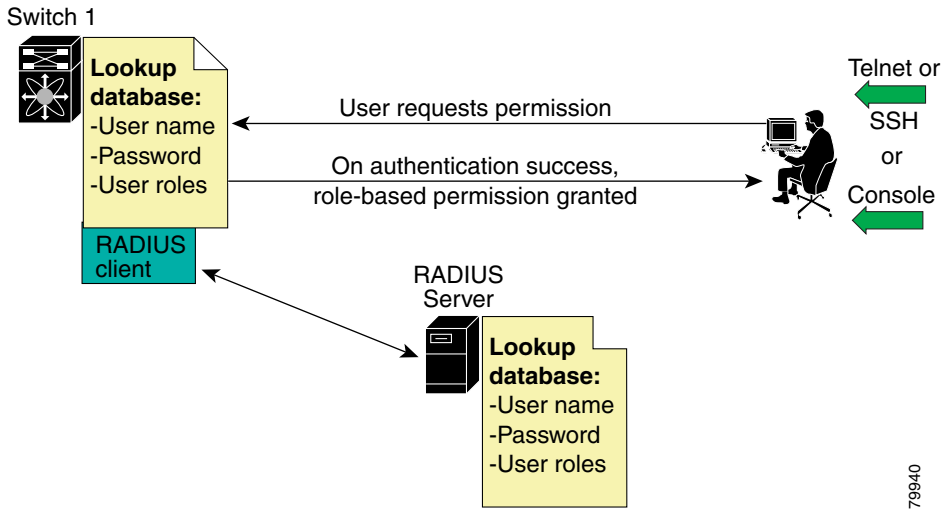


RADIUS Authentication

Cisco MDS 9000 Family switches provide remote authentication through RADIUS servers. You can also configure multiple RADIUS servers, and each server is tried in the order specified.

RADIUS protocols support one-time password (OTP) schemes that all switches can make use of for authentication purposes (see Figure 14-2).

Figure 14-2 RADIUS Authentication



Role-Based Authorization

By default, two roles exist in all switches:

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

The two default roles cannot be changed or deleted. Vendor-specific attributes (VSAs) contain the user profile information used by the switch. To use this option, configure the VSAs on the RADIUS servers.

Accounting

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

Authentication and Authorization Process

The following steps explain the authorization and authentication process. Figure 14-3 shows a flow chart of the process.

Step 1 The switch software receives your user ID and password through a console or Telnet (or SSH) application.

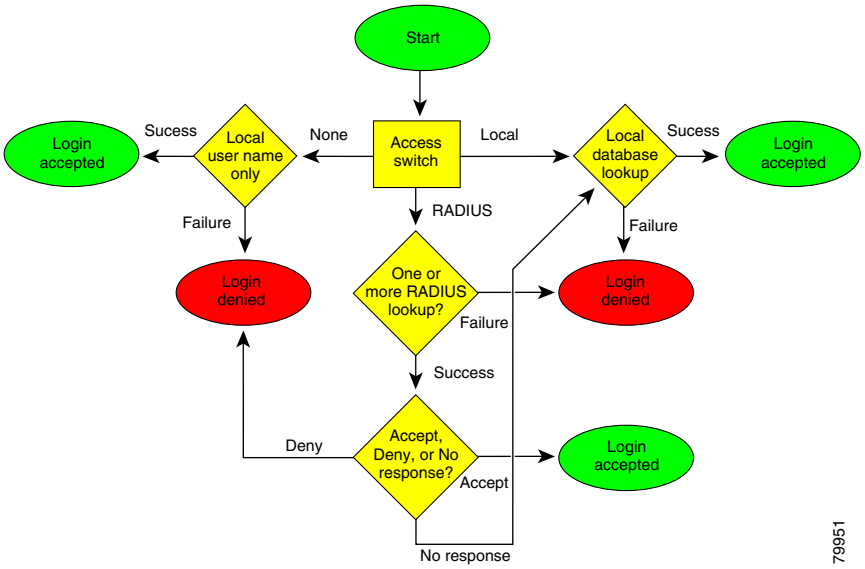
Step 2 The remote server is contacted if remote authentication is enabled, or else local authentication is performed.

Note If remote authentication is enabled but none of the servers are available (network failure), local authentication is performed.

Step 3 If authentication is successful, you are given access to the switch with appropriate permissions based on the roles to which you belong. These roles can be configured locally or can be sent by the remote server during the authentication process.

Step 4 If remote authentication is rejected, you are denied access and an appropriate message is issued.

Figure 14-3 Switch Authorization and Authentication Flow



Configuring CLI Authentication Methods

You can configure remote and local authentication for Telnet, SSH, or console access. These commands are restricted to privileged users as determined by your administrator.

Setting AAA Authentication

You can individually set authentication options for console or Telnet (and SSH) access using the **aaa authentication login** command. Local authentication is always disabled by default (see the "Authentication and Authorization Process" section on page 14-4).

To configure the authentication option, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# aaa authentication login radius telnet` `switch(config)#`	Enables Telnet authentication (and SSH) to use RADIUS.
	`switch(config)# aaa authentication login radius console` `switch(config)#`	Enables console authentication to use RADIUS.
	`switch(config)# aaa authentication login local telnet` **Note** This command applies to both Telnet and SSH.	Enables only local authentication for Telnet (and SSH) access. The **local** option disables other authentication methods and configures local authentication to be used exclusively.
	`switch(config)# aaa authentication login none console`	Disables authentication for console access. User name authentication is still done.

Enabling or Disabling Telnet Access

You can use the **telnet server enable** command to enable Telnet access to the switch. By default, this service is enabled.

To enable or disable Telnet access to the switch, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# telnet server enable` `switch(config)#`	Turns on Telnet access to the switch.
	`switch(config)# no telnet server enable` `switch(config)#`	Turns off Telnet access to the switch.

Displaying CLI Authentication Commands

The **show authentication** command displays the configured authentication methods. See Example 14-1.

Example 14-1 Displays Authentication Information

```
switch# show authentication
authentication method:none
         console:not enabled
         telnet/ssh:not enabled
authentication method:radius
         console:not enabled
         telnet/ssh:not enabled
authentication method:local
         console:enabled
         telnet/ssh:enabled
```

The **show telnet server** command displays the state of the Telnet access configuration. See Example 14-2.

Example 14-2 Displays Telnet Server Details

```
switch# show telnet server
telnet service enabled
```

Configuring Role-Based CLI Authorization

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

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

To configure a new role or to modify the profile for an existing role, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# role name techdocs` `switch(config-role)#`	Places you in the mode for the specified role (techdocs). **Note** The role submode prompt indicates that you are now in the role submode. This submode is now specific to the techdocs group.
	`switch(config)# no role name techdocs`	Deletes the role called techdocs.
Step 3	`switch(config-role)# description Entire Tech. Docs. group`	Assigns a description to the new role. The description is limited to one line and can contain spaces.
	`switch(config-role)# no description`	Resets the description for the Tech. Docs. group.

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

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

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

Configuring Rules and Features for Each Role

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

The user-specified rule number determines the order in which the rules are applied. For example, rule 1 is applied before rule 2 which is applied before rule 3 etc.

Note In this case, **exec** commands refer to all commands in the EXEC mode that do not fall in the **show**, **debug**, and **clear**, categories. Up to 16 rules can be configured for each role.

To configure a new role or to modify the profile for an existing role, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# role name sangroup` `switch(config-role)#`	Places you in *sangroup* role submode.

Step 3	`switch(config-role)# rule 1 permit config`
	`switch(config-role)# rule 2 deny config feature fspf`
	`switch(config-role)# rule 3 permit debug feature zone`
	`switch(config-role)# rule 4 permit exec feature fcping`
		Allows users belonging to the *sangroup* role to perform all configuration commands except f**spf config** commands. They can also perform **zone debug** commands and the **fcping** EXEC mode command.

Step 4	`switch(config-role)# no rule 4`	Deletes rule 4 which no longer permits the *sangroup* to perform the **fcping** command.

In Step 3, rule 1 is applied first, thus permitting all **config** commands to sangroup users. Rule 2 is applied next, denying FSPF configuration to sangroup users. As a result, sangroup users can perform all other **config** commands, except **fspf** configuration commands.

Note The order of rule placement is important. If you had swapped these two rules and issued the **deny config feature fspf** rule first and issued the **permit config** rule next, you would be allowing all sangroup users to perform all configuration commands since the second rule globally overrode the first rule.

Configuring the VSAN Policy

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

To configure a new role or to modify the VSAN policy for an existing role, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# role name sangroup` `switch(config-role)#`	Places you in *sangroup* role submode.
Step 3	`switch(config)# vsan policy deny` `switch(config-role-vsan)`	Changes the VSAN policy of this role to **deny** and places you in a submode where VSANs can be selectively permitted.
	`switch(config-role)# no vsan policy deny`	Deletes the configured VSAN role policy and reverts to the factory default (**permit**).

	Command	Purpose
Step 4	`switch(config-role-vsan)# permit vsan 10-30`	Permits this role to perform the allowed commands for VSANs 10 through 30.
	`switch(config-role-vsan)# no permit vsan 15-20`	Removes the permission for this role to perform commands for vsan 15 to 20. So, the role is now permitted to perform commands for VSAN 10 to 14, and 21 to 30.

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

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

Displaying Role-Based CLI Information

Use the **show role** command to display rules configured on the switch including those rules that have not yet been committed to persistent storage. The rules are displayed by rule number and are based on each role. All roles are displayed even if role name is not specified. See Example 14-3.

Example 14-3 Displays Information for All Roles

```
switch# show role
Role: network-admin
Description: Predefined Network Admin group. This role cannot be modified
Access to all the switch commands

Role: network-operator
Description: Predefined Network Operator group. This role cannot be modified
Access to Show commands and selected Exec commands

Role: TechDocs
vsan policy: permit (default)

Role: sangroup
Description: SAN management group
vsan policy: deny
Permitted vsans: 10-30

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

Configuring CLI User Profiles

Every Cisco MDS 9000 Family switch user has related NMS information stored by the system. Your authentication information, user name, user password, password expiration date, and role membership are stored in your user profile. The CLI commands explained in this section enable you to create users and modify the profile of an existing user.These commands are restricted to privileged users as determined by your administrator.

Creating or Updating Users

The switches use the same command (**username**) to create a user and to update an existing user. The **expire** option determines the date on which the user account is disabled. The date is specified in the YYYY-MM-DD format. By default, the user account does not expire unless you explicitly configure it to expire.

Tip The following words are reserved and cannot be used to configure users: bin, daemon, adm, lp, sync, shutdown, halt, mail, news, uucp, operator, games, gopher, ftp, nobody, nscd, mailnull, rpc, rpcuser, xfs, gdm, mtsuser, ftpuser, man, and sys

Note User passwords are not displayed in the switch configuration file.

To configure a new user or to modify the profile of an existing user, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# username usam password abcd expire 2003-05-31`	Creates or updates the user account (usam) along with a password (abcd) that is set to expire on 2003-05-31. The password is limited to 64 characters.
	`switch(config)# username msam password 0 abcd role network-operator`	Creates or updates the user account (msam) along with a password (abcd) specified in clear text (indicated by 0). The password is limited to 64 characters.
	`switch(config)# username user1 password 5 !@*asdsfsdfjh!@df`	Specifies an encrypted (specified by 5) password (!@*asdsfsdfjh!@df) for the user account (user1).
Step 3	`switch(config)# username usam role network-admin`	Adds the specified user (usam) to the network-admin role.
	`switch(config)# no username usam role vsan-admin`	Deletes the specified user (usam) from the vsan-admin role.
Step 4	`switch(config)# username usam sshkey fsafsd2344234234ffgsdfg`	Identifies the contents of the SSH key for the specified user (usam).
	`switch(config)# no username usam sshkey fsafsd2344234234ffgsdfgffsdfsfsfssf`	Deletes the SSH key content identification for the user (usam).

Note If the **update-snmpv3** option is used, specify the clear text and old SNMP password (see the "Forcing Identical SNMP and CLI Passwords" section on page 14-25).

Logging out CLI Users

To log out another user on the switch, use the **clear user** command.

```
switch# clear user vsam
switch#
```

In this example, the user named vsam is logged out from the switch.

Displaying User Profile Information

Use the **show user-account** command to display configured information about user accounts. See Examples 14-4 to 14-6.

Example 14-4 Displays All Users

```
switch# show users
admin    pts/7        Jan 12 20:56 (10.77.202.149)
admin    pts/9        Jan 12 23:29 (modena.cisco.com)
admin    pts/10       Jan 13 03:05 (dhcp-171-71-58-120.cisco.com)
admin    pts/11       Jan 13 01:53 (dhcp-171-71-49-49.cisco.com)
```

Example 14-5 Displays Information for a Specified User

```
switch# show user-account user1
user:user1
        this user account has no expiry date
        roles:network-operator
no password set. Local login not allowed
Remote login through RADIUS is possible
```

Example 14-6 Displays Information for All Users

```
switch# show user-account
show user-account
user:admin
        this user account has no expiry date
        roles:network-admin
user:usam
        expires on Sat May 31 00:00:00 2003
        roles:network-admin network-operator
user:msam
        this user account has no expiry date
        roles:network-operator
user:user1
        this user account has no expiry date
        roles:network-operator
no password set. local login not allowed
Remote login through RADIUS is possible
```

Configuring CLI Accounting Parameters

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 purposes and user accountability. Accounting can be implemented locally or remotely (using RADIUS).

Setting the Accounting Log Size

The **aaa accounting logsize** command sets the size limit of the accounting log file in persistent storage. The default is 15,000 bytes.

To set the log file size, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# aaa accounting logsize 29000`	Sets the size of the log file on the local disk. The default is 15,000 bytes.

Enabling RADIUS Accounting

To enable RADIUS accounting in a switch, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# aaa accounting method radius`	Configures the RADIUS accounting method on the switch. By default, only local accounting is enabled.

You can clear the RADIUS accounting configuration by issuing the **no aaa accounting method radius** command.

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* flag in the AAA client configuration. This flag should be turned on 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.

Displaying Accounting Configuration

The **show accounting** command displays configured accounting information. See Examples 14-7 to 14-9.

Example 14-7 Displays Configured Accounting Parameters.

```
switch# show accounting config
RADIUS accounting not enabled
local accounting enabled
```

Example 14-8 Displays Configured Log Size.

```
switch# show accounting logsize
maximum local accounting log size:29000
```

Example 14-9 Displays the Entire Log File.

```
switch# show accounting log
Tue Jan 15 06:03:24 1980:update:::Created interface vsan1

Tue Jan 15 06:15:08 1980:start:/dev/pts/0_316764908:admin
Tue Jan 15 07:26:10 1980:stop:/dev/pts/0_316764908:admin:vsh exited normally
Tue Jan 15 07:46:40 1980:update:/dev/ttyS0_316753046:admin:Alias test is created
 on VSAN 1

Tue Jan 15 07:46:40 1980:update:/dev/ttyS0_316753046:admin:Alias test is removed
 on VSAN 1

Tue Jan 15 08:01:57 1980:update:/dev/ttyS0_316753046:admin:in-order delivery gua
rantee settings changed in-order guarantee:yes
Tue Jan 15 08:02:31 1980:update:/dev/ttyS0_316753046:admin:Enabled IP routing

Tue Jan 15 08:09:51 1980:update:/dev/ttyS0_316753046:admin:Alias test is created
 on VSAN 1

Tue Jan 15 08:09:52 1980:update:/dev/ttyS0_316753046:admin:Alias test is removed
 on VSAN 1

Tue Jan 15 08:11:30 1980:update:/dev/ttyS0_316753046:admin:Zone test is created
on VSAN 1
.
.
.
Sat Jan 19 22:16:06 1980:update:/dev/pts/0_317167691:admin:Zone cisco is removed
 on VSAN 1

Sat Jan 19 22:56:49 1980:stop:/dev/pts/0_317167691:admin:vsh exited normally
Sun Jan 20 17:07:50 1980:start:snmp_317236070_10.77.202.149:public
Sun Jan 20 17:07:50 1980:stop:snmp_317236070_10.77.202.149:public:
Mon Jan 21 03:38:03 1980:start:/dev/pts/0_317273883:admin
Mon Jan 21 04:08:25 1980:stop:/dev/pts/0_317273883:admin:vsh exited normally
Mon Jan 21 06:43:49 1980:start:/dev/pts/0_317285029:admin
Mon Jan 21 06:44:38 1980:stop:/dev/pts/0_317285029:admin:vsh exited normally
Mon Jan 21 07:24:16 1980:start:/dev/pts/0_317287456:admin
```

Recovering Administrator Password

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

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

- Physically remove the other supervisor module from the chassis, or
- Change the other supervisor module's console prompt to the `loader>` or `switch(boot)#` prompt (see the "Recovery from the loader> Prompt" section on page 5-35) until you complete this procedure.

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

To recover a administrator's password, follow these steps:

Step 1 Reboot the switch.

```
switch# reload
The supervisor is going down for reboot NOW!
```

Step 2 Press the **Ctrl-]** key sequence (when the switch begins its SAN-OS software boot sequence) to enter the `switch(boot)#` prompt (see "Recovery Interruption" section on page 5-31).

```
Ctrl-]
switch(boot)#
```

Step 3 Change to configuration mode.

```
switch(boot)# config terminal
```

Step 4 Enter the **admin-password** command to reset the administrator password.

```
switch(boot-config)# admin-password password
```

Step 5 Exit to the EXEC mode.

```
switch(boot-config)# exit
switchboot#
```

Step 6 Enter the **load** command to load the SAN-OS software.

```
switch(boot)# load bootflash:system.img
```

Step 7 Save the software configuration.

```
switch# copy running-config startup-config
```

Configuring RADIUS Authentication

You can configure RADIUS query parameters. These commands are restricted to privileged users as determined by your administrator.

Setting the RADIUS Server Address

You can add up to five (5) RADIUS servers using the **radius-server host** command. You can configure a RADIUS server to be a primary server so it is always contacted first. If you have not configured a primary server, the RADIUS servers are tried in the order they were configured.

To specify the RADIUS server address and the 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 primary` `switch(config)#`	Adds 10.10.0.0 users to the RADIUS server list as the primary server. This server is always tried first.
Step 3	`switch(config)# radius-server host 10.10.0.0 key HostKey` `switch(config)#`	Specifies a 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 4	`switch(config)# radius-server host 10.10.0.0 auth-port 2003` `switch(config)#`	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.
Step 5	`switch(config)# radius-server host 10.10.0.0 acct-port 2004` `switch(config)#`	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 6	`switch(config)# radius-server host 10.10.0.0 accounting` `switch(config)#`	Specifies this server to be used only for accounting purposes. **Note** If neither the **authentication** option nor the **accounting** options are specified, the server is used for both accounting and authentication purposes.
Step 7	`switch(config)# radius-server host radius1 primary` `switch(config)#`	Specifies the server to be the primary server.
	`switch(config)# radius-server host radius2 key 0 abcd` `switch(config)#`	Specifies a clear text key for the specified server. The key is restricted to 65 characters.
	`switch(config)# radius-server host radius3 key 7 1234` `switch(config)#`	Specifies a reversible encrypted key for the specified server. The key is restricted to 65 characters.

Setting the RADIUS Preshared Key

You need to configure the RADIUS preshared key to authenticate the switch to the RADIUS server. The length of the key is restricted to 65 characters and can include any printable ASCII characters (white spaces are not allowed). You can configure a global key to be used for all RADIUS server configurations on the switch. You can override this global key assignment by explicitly using the **key** option in the **radius-server host** command.

To set 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` `switch(config)#`	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` `switch(config)#`	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 public` `switch(config)#`	Configures a preshared key (public) specified in encrypted text (indicated by 7) to authenticate communication between the RADIUS client and server.

Setting the RADIUS Server Time-Out Interval

To specify the time 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` `switch(config)#`	Specifies the time (in seconds) between retransmissions to the RADIUS server. The default time-out is one (1) second. The time range in seconds is 1 to 60.

You can revert the retransmission time to its default by issuing the **no radius-server timeout** command.

Setting Iterations of the RADIUS Server

By default, a switch retries a RADIUS server connection only once. This number can be configured. The maximum is five retries per server. You can revert the retry number to its default by issuing the **no radius-server retransmit** command.

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` `switch(config)#`	Configures the number of times (3) the switch tries to connect to a RADIUS server(s) before reverting to local authentication.

The worst case cumulative response or timeout latency from RADIUS servers for authentication should not be more than 50 sec. For example in the following configuration:

```
radius-server timeout 5
radius-server retransmit 3
radius-server host A authentication
radius-server host B authentication
```

The worst case cumulative response or timeout latency will be:

```
(5+1)*3   +     (5+1)*3 = 36
^^^^^^^^        ^^^^^^^^^  ^^^^^
server A        server B   total
```

Note You need to add one (1) to the retransmit count to calculate the total. The total number of tries equals the number of retransmits + 1.

Defining Vendor-Specific Attributes

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

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

Where `protocol` is a Cisco attribute for a particular type of authorization, and `sep` is `=` for mandatory attributes, and `*` is for optional attributes.

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

VSA Format

The following VSA protocol options are supported:

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

The following attributes are supported:

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

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

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

Authorization Process

The RADIUS based authorization process is as follows:

Step 1 The switch sends an Access-Request packet to the RADIUS server.

Step 2 The RADIUS server responds with an Accept or Reject message.

- If Access-Reject is received, that means authentication has failed and no authorization information is sent.
- If Access-Accept is received, that means authentication is successful and VSA is also sent along with the Access-Accept packet.
- If no VSA data is sent, local authorization is used.
- If your user name has no corresponding local account, a new account is created. This new account is locked and cannot be used for local login. It is deleted after 24 hours.

Step 3 You are made a member of all groups indicated in the role list attribute in the VSA. You are removed from those roles if your role is not listed in the VSA group list.

Displaying RADIUS Server Details

Use the **show radius-server** command to display all configured RADIUS server parameters (see Example 14-10).

Note Only administrators can view the RADIUS preshared key.

Example 14-10 Displays Configured RADIUS Information

```
switch# show radius-server
Global RADIUS shared secret:Myxgqc
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:23MHcUnD
        10.10.0.0:
                available for authentication on port:1812
                available for accounting on port:1813
                RADIUS shared secret:hostkey----> for administrators only
```

Configuring SSH Services

The Telnet service is enabled by default on all Cisco MDS 9000 Family switches. Before enabling the SSH service, generate a host key pair. To generate a host key, use the **ssh key** command (see the "Generating an SSH Host Key Pair" section on page 14-20).

Enabling SSH Service

By default, the SSH service is disabled. To enable SSH service, issue the **ssh server enable** command.

To enable or disable the SSH service, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# ssh server enable` `updated`	Enables the use of the SSH service.
	`switch(config)# no ssh server enable` `updated`	Disables (default) the use of the SSH service and resets the switch to its factory defaults.

Generating an SSH Host Key Pair

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

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

To generate the SSH host key pair, follow these steps:

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

Step 2	`switch(config)# ssh key rsa1 1024`
	`generating rsa1 key.....`
	`generated rsa1 key`
	`switch(config)#`
		Generates the RSA1 host key pair.

	`switch(config)# ssh key dsa 1024`
	`generating dsa key.....`
	`generated dsa key`
	`switch(config)#`
		Generates the DSA host key pair.

	`switch(config)# ssh key rsa 1024`
	`generating rsa key.....`
	`generated rsa key`
	`switch(config)#`
		Generates the RSA host key pair.

	`switch(config)# no ssh key rsa 1024`
	`cleared RSA keys`
	`switch(config)#`
		Clears the RSA host key pair configuration.
		Caution If you delete all of the SSH keys, you cannot start a new session.

Using the force Option

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

To overwrite the previously generated key pair, follow these steps:

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

Step 2	`switch(config)# ssh key dsa 768`
	`ssh key dsa 512`
	`dsa keys already present, use force`
	`option to overwrite them`
	`switch(config)# ssh key dsa 512 force`
	`deleting old dsa key.....`
	`generating dsa key.....`
	`generated dsa key`
	`switch(config)#`
		Tries to set the host key pair. If a required host key pair is already configured, use the **force** option to overwrite that host key pair.
		Deletes the old DSA key and sets the host key pair using the new bit specification.

Clearing SSH Hosts

To manually clear trusted SSH host entries, issue the **clear ssh hosts** command at the switch prompt:

Example 14-11 Clearing Configured SSH Hosts

```
switch# clear ssh hosts
switch#
```

This command clears all SSH hosts.

Displaying SSH Protocol Status

Use the **show ssh server** command to display the status of the SSH protocol (enabled or disabled) and the versions that are enabled for that switch. See Example 14-12.

Example 14-12 Displays SSH Protocol Status

```
switch# show ssh server
ssh is enabled
version 1 enabled
version 2 enabled
```

Use the **show ssh key** command to display the host key pair details for the specified key or for all keys, if no key is specified. See Example 14-13.

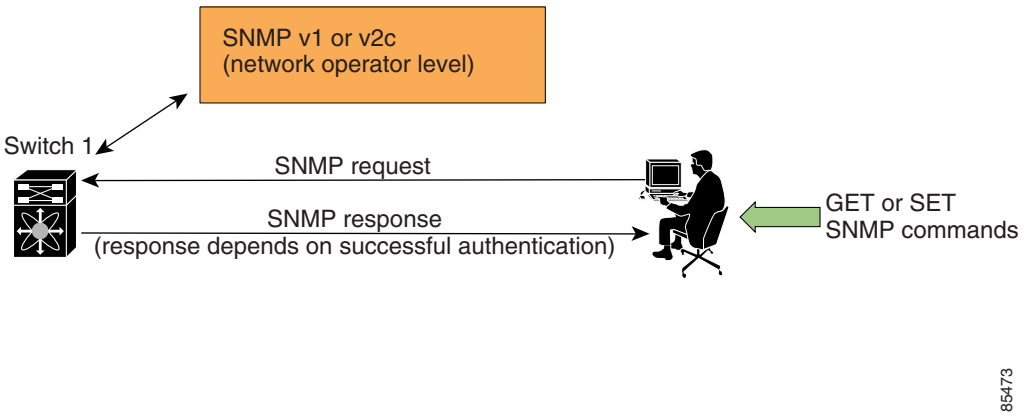
Example 14-13 Displays Host Key Pair Details

```
switch# show ssh key
rsa1 Keys generated:Sun Jan 13 07:16:26 1980
1024 35
fingerprint:
1024 67:76:02:bd:3e:8d:f5:ad:59:5a:1e:c4:5e:44:03:07
could not retrieve rsa key information
dsa Keys generated:Sun Jan 13 07:40:08 1980
ssh-dss AAAAB3NzaC1kc3MAAABBAJTCRQOydNRel2v7uiO6Fix+OTn8eGdnnDVxw5eJs5OcOEXOyjaW
cMMYsEgxc9ada1NElp8Wy7GPMWGOQYj9CU0AAAAVAMCcWhNN18zFNOIPo7cU3t7d0iEbAAAAQBdQ8UAO
i/Cti84qFb3kTqXlS9mEhdQUo0lHcH5bw5PKfj2Y/dLR437zCBKXetPj4p7mhQ6Fq5os8RZtJEyOsNsA
AABAA0oxZbPyWeR5NHATXiyXdPI7j9i8fgyn9FNipMkOF2Mn75Mi/lqQ4NIq0gQNvQOx27uCeQlRts/Q
wI4q68/eaw==
fingerprint:
512 f7:cc:90:3d:f5:8a:a9:ca:48:76:9f:f8:6e:71:d4:ae
```

SNMP Security

SNMP is an application layer protocol that facilitates the exchange of management information between network devices. In all Cisco MDS 9000 Family switches, three SNMP versions are available: SNMPv1, SNMPv2c, and SNMPv3 (see Figure 14-4).

Figure 14-4 SNMP Security



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

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

SNMP Version 1 and Version 2c

SNMPv1 and SNMPv2c use a community string match for user authentication. Community strings provided a weak form of access control in earlier versions of SNMP. SNMPv3 provides much improved access control using strong authentication and should be preferred over SNMPv1 and SNMPv2c wherever it is supported.

SNMP Version 3

SNMPv3 is an interoperable standards-based protocol for network management. SNMPv3 provides secure access to devices by a combination of authenticating and encrypting frames over the network. The security features provided in SNMPv3 are:

- Message integrity—Ensures that a packet has not been tampered with in-transit.
- Authentication—Determines the message is from a valid source.
- Encryption—Scrambles the packet contents to prevent it from being seen by unauthorized sources.

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

Restricting Switch Access

You can restrict access to a Cisco MDS 9000 Family switch using IP Access Control Lists (IP-ACLs). See the "IP Access Control Lists" section on page 17-5.

Group-Based SNMP Access

Note Because *group* is a standard SNMP term used industry-wide, we refer to role(s) as group(s) in this SNMP section.

SNMP access rights are organized by groups. Each group in SNMP is similar to a role through the CLI. Each group is defined with three accesses: read access, write access, and notification access. Each access can be enabled or disabled within each group.

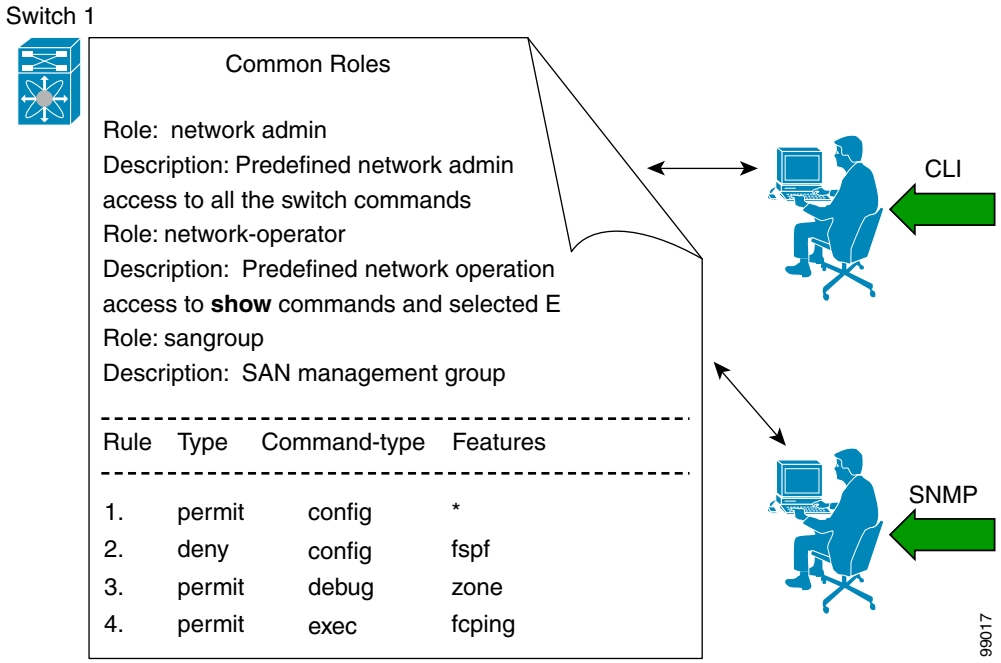
You can begin communicating with the agent once the your user name is created, your roles are set up by your administrator, and you are added to the roles.

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

Configuring Common Roles

From Release 1.2(x), CLI and SNMP in all switches in the Cisco MDS 9000 Family use the common roles database. This database contains any role that is created using CLI or SNMP. You can use SNMP to modify a role that was created using CLI and vice versa (see Figure 14-5).

Figure 14-5 Common Roles Database



Each role in SNMP is the same as a role created or modified through the CLI (see "Configuring Role-Based CLI Authorization" section on page 14-7).

Each role in the Common Role database can be restricted to one or more VSAN as required.

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

- SNMP—Use the CISCO-COMMON-ROLES-MIB to configure or modify roles in the common roles database. Refer to the *Cisco MDS 9000 Family MIB Reference Guide* for more information.
- CLI—Use the **role name** command.

Creating and Modifying Users

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

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

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

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

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

By default only two roles are available in a Cisco MDS 9000 Family switch—network-operator and network-admin. You can also use any role that is configured in the Common Roles database (see the "Configuring Common Roles" section on page 14-23).

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

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# snmp-server user joe network-admin auth sha abcd1234`	Creates or modifies the settings for a user (joe) in the network-admin role using the HMAC-SHA-96 authentication password (abcd1234).
	`switch(config)# snmp-server user sam network-admin auth md5 abcdefgh` `switch(config)#`	Creates or modifies the settings for a user (sam) in the network-admin role using the HMAC-MD5-96 authentication password (abcdefgh).
	`switch(config)# snmp-server user Bill network-admin auth sha abcd1234 priv abcdefgh`	Creates or modifies the settings for a user (network-admin) in the network-admin role using the HMAC-SHA-96 authentication level and privacy encryption parameters.
	`switch(config)# no snmp-server user usernameA`	Deletes the user (usernameA) and all associated parameters.
	`switch(config)# snmp-server user user1 network-admin auth md5 0xab0211gh priv 0x45abf342 localizedkey`	Specifies the password to be in localized key format (see RFC2574). The localized key is provided in the hex format (for example, 0xacbdef).

Note Avoid using the **localizedkey option** when configuring an SNMP user from CLI. The localized keys are not portable across devices as they contain device engine ID information. If a configuration file is copied to the device, the passwords may not be set correctly if the configuration file was generated at a different device. Explicitly configure the desired passwords after copying the configuration into the device.

Forcing Identical SNMP and CLI Passwords

You can force the SNMPv3 password and the CLI password to be the same. You must know the SNMPv3 password to change the password using the CLI. Use CLI password to synchronize the SNMP password The password is limited to a minimum of 8 characters and a maximum of 64 characters.

Caution To change the SNMP password, a clear text CLI password is required.

To modify the secret key for an SNMPv3 user, refer to RFC2574.

To update the SNMPv3 password from the CLI, follow these steps:

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# username joe password wxyz6789 update-snmpv3 abcd1234`	Updates the SNMPv3 password for the specified user (joe). The local CLI password and the SNMP password are updated. If user Joe does not exist, the command fails.

Assigning Users to Roles

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

To assign users to roles through SNMP, refer to RFC2575.

To assign users to roles through the CLI, refer to the procedure specified in the "Creating and Modifying Users" section on page 14-24.

Adding or Deleting Communities

You can configure read-only or read-write access for SNMP users by using the **snmp-server community** CLI command. Use the **no** form of the command to delete the configured community. Refer to RFC2576.

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

	Command	Purpose
Step 1	`switch# config t`	Enters configuration mode.
Step 2	`switch(config)# snmp-server community snmp_Community ro`	Adds read-only access for the specified SNMP community.
	`switch(config)# snmp-server community snmp_Community rw`	Adds read-write access for the specified SNMP community.
	`switch(config)# no snmp-server community snmp_Community`	Deletes access for the specified SNMP community (default).

Displaying SNMP Security Information

Use the **show snmp** commands to display configured SNMP information (see Example 14-14 and 14-16).

Example 14-14 Displays SNMP User Details

```
switch# show snmp user
User                          Group                         Auth  Priv
____                          _____                         ____  ____
steve                         network-admin                 md5   des
sadmin                        network-admin                 md5   des
stever                        network-operator              md5   des
```

Example 14-15 Displays SNMP Community Information

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

Example 14-16 Displays SNMP Host Information

```
switch# show snmp host
Host                           Port Version  Level  Type   SecName
____                           ____ _______  ______ ____   _______
171.16.126.34                  2162 v2c      noauth trap   public
171.16.75.106                  2162 v2c      noauth trap   public
...
171.31.58.97                   2162 v2c      auth   trap   public
...
```

Displaying SNMP Counter Information

The **show snmp** command displays counter information for SNMP contact, location, and packet settings. This command provides information that is used entirely by the Cisco MDS 9000 Family Fabric Manager (refer to the *Cisco MDS 9000 Family Fabric Manager User Guide*). See Example 14-17.

Example 14-17 Displays SNMP

```
switch# show snmp
switch# show snmp
sys contact:
sys location:
1631 SNMP packets input
        0 Bad SNMP versions
        0 Unknown community name
        0 Illegal operation for community name supplied
        0 Encoding errors
        64294 Number of requested variables
        1 Number of altered variables
        1628 Get-request PDUs
        0 Get-next PDUs
        1 Set-request PDUs
152725 SNMP packets output
```

```
        0 Too big errors
        1 No such name errors
        0 Bad values errors
        0 General errors
Community                      Access
---------                      ------
public                          rw
User                          Group                          Auth  Priv
____                          _____                          ____  ____
admin                         network-admin                  md5   no
```

Default Security Settings

Table 14-2 lists the default settings for all security features in any switch.

Table 14-2 Default Security Settings

Parameters	Default
Roles in each switch (for CLI and SNMP users)	Two default roles—network-operator and network-admin.
AAA authentication login	Local authentication is enabled. If the Telnet or SSH options are not specified, the command applies to both.
Telnet server	Enabled.
Accounting log file size on local disk	15,000 bytes.
User's account expiration	Does not expire unless you explicitly configure it to expire.
RADIUS server timeout interval	The default time-out is five (5) seconds.
RADIUS preshared key	No key is configured.
RADIUS server connection attempts	A switch tries to connect to a RADIUS server up to 3 times.
RADIUS Authentication messages	1812 messages sent by destination UDP port.
RADIUS Accounting messages	1813 messages sent by destination UDP port.
User name	admin.
User password	admin.