CHAPTER 17

Troubleshooting RADIUS and TACACS+

The authentication, authorization, and accounting (AAA) mechanism verifies the identity of, grants access to, and tracks the actions of users managing a switch. All Cisco MDS 9000 Family switches use the Remote Access Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) protocols to provide solutions using remote AAA servers.

This chapter includes the following sections:

AAA Overview

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 AAA server(s). A preshared secret key provides security for communication between the switch and AAA servers. This secret key can be configured as a global key for all AAA servers or on a per AAA server basis. This security mechanism provides a central management capability for AAA servers.

Note Users authenticated through a remote AAA server cannot create jobs using the command scheduler.

Initial Troubleshooting Checklist

Begin troubleshooting AAA issues by checking the following issues:

Checklist	Check off
Use the **test aaa server** CLI command to verify connectivity to your AAA server.	❑
Verify that you have assigned appropriate attributes on your AAA server for user roles.	❑
Verify that the preshared key is the same on both the switch and the AAA server.	❑
Verify that you have no all-numeric users or passwords configured.	❑

Common Troubleshooting Tools in Fabric Manager

Use the following Fabric Manager procedures to troubleshoot AAA issues:

- Choose **Switches > Security > AAA > RADIUS** to view the RADIUS configuration.
- Choose **Switches > Security > AAA > TACACS+** to view the TACACS+ configuration.
- Choose **Switches > Security > AAA** to view server group and AAA monitor deadtime values.

Common Troubleshooting Commands in the CLI

Use the following CLI commands to troubleshoot AAA issues:

- **show aaa authentication**
- **show user-account**
- **show radius status**
- **show radius-server**
- **show tacacs+ status**
- **show tacacs-server**

Use the following **debug** commands to determine the root cause of an issue:

- **debug radius aaa-request**
- **debug radius aaa-request-lowlevel**
- **debug tacacs+ aaa-request and**
- **debug tacacs+ aaa-request-lowlevel**

AAA Issues

This section describes common AAA issues and includes the following topics:

Switch Does Not Communicate with AAA Server

Multiple misconfigurations can result in an AAA server that the Cisco SAN-OS switch does not communicate with.

Symptom Switch does not communicate with AAA server.

Table 17-1 Switch Does Not Communicate with AAA Server

Symptom	Possible Cause	Solution
Switch does not communicate with AAA server.	Incorrect authentication or accounting port configured.	Reconfigure the authentication or accounting ports to match those configured on the AAA server. For RADIUS servers, see the "Verifying RADIUS Configuration Using Fabric Manager" section on page 17-4 or the "Verifying RADIUS Configuration Using the CLI" section on page 17-4. For TACACS+ servers, see the "Verifying TACACS+ Configuration Using Fabric Manager" section on page 17-5 or the "Verifying TACACS+ Configuration Using the CLI" section on page 17-5.
	Incorrect preshared key configured.	Reconfigure the same preshared key on the switch and the AAA server. For RADIUS servers, see the "Verifying RADIUS Configuration Using Fabric Manager" section on page 17-4 or the "Verifying RADIUS Configuration Using the CLI" section on page 17-4. For TACACS+ servers, see the "Verifying TACACS+ Configuration Using Fabric Manager" section on page 17-5 or the "Verifying TACACS+ Configuration Using the CLI" section on page 17-5.
	AAA server monitor deadtime set to high.	Set the deadtime lower to bring AAA servers active more quickly. For RADIUS servers, see the "Verifying RADIUS Server Monitor Configuration Using Fabric Manager" section on page 17-6 or the "Verifying RADIUS Server Monitor Configuration Using the CLI" section on page 17-6. For TACACS+ servers, see the "Verifying TACACS+ Server Monitor Configuration Using Fabric Manager" section on page 17-7 or the "Verifying TACACS+ Server Monitor Configuration Using the CLI" section on page 17-7.
	Timeout value too low.	Change server timeout value to ten seconds or higher. For RADIUS servers, see the "Verifying RADIUS Server Monitor Configuration Using Fabric Manager" section on page 17-6 or the "Verifying RADIUS Server Monitor Configuration Using the CLI" section on page 17-6. For TACACS+ servers, see the "Verifying TACACS+ Server Monitor Configuration Using Fabric Manager" section on page 17-7 or the "Verifying TACACS+ Server Monitor Configuration Using the CLI" section on page 17-7.

Verifying RADIUS Configuration Using Fabric Manager

To verify or change the RADIUS configuration using Fabric Manager, follow these steps:

Step 1 Choose **Switches > Security > AAA > RADIUS** and select the **Servers** tab. You see the RADIUS configuration in the Information pane.

Step 2 Highlight the server that you need to change and click **Delete Row** to delete this server configuration.

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

Step 4 Set the KeyType and Key fields to the preshared key configured on the RADIUS server.

Step 5 Set the AuthPort and AcctPort fields to the authentication and accounting ports configured on the RADIUS server.

Step 6 Set the TimeOut value and click **Apply** to save these changes.

Step 7 Select the **CFS** tab and select **commit** from the Config Action drop-down menu and click **Apply Changes** to distribute these changes to all switches in the fabric.

Verifying RADIUS Configuration Using the CLI

To verify or change the RADIUS configuration using the CLI, follow these steps:

Step 1 Use the **show radius-server** command to display configured RADIUS parameters.

```
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
        10.1.1.1:
                available for authentication on port:1812
                available for accounting on port:1813
                RADIUS shared secret:******
        10.2.2.3:
                available for authentication on port:1812
                available for accounting on port:1813
                RADIUS shared secret:******
```

Step 2 Use the **radius-server host** *ip-address* **key** command to set the preshared key to match what is configured on your RADIUS server.

Step 3 Use the **radius-server host** *ip-address* **auth-port** command to set the authentication port to match what is configured on your RADIUS server.

Step 4 Use the **radius-server host** *ip-address* **acc-port** command to set the accounting port to match what is configured on your RADIUS server.

Step 5 Use the **radius-server timeout** command to set the period in seconds for the switch to wait for a response from all RADIUS servers before the switch declares a timeout failure.

Step 6 Use the **radius commit** command to commit any changes and distribute to all switches in the fabric.

Verifying TACACS+ Configuration Using Fabric Manager

To verify or change the TACACS+ configuration using Fabric Manager, follow these steps:

Step 1 Choose **Switches > Security > AAA > TACACS+** and select the **Servers** tab. You see the TACACS+ configuration in the Information panel.

Step 2 Highlight the server that you need to change and click **Delete Row** to delete this server configuration.

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

Step 4 Set the KeyType and Key fields to the preshared key configured on the TACACS+ server.

Step 5 Set the AuthPort and AcctPort fields to the authentication and accounting ports configured on the TACACS+ server.

Step 6 Set the TimeOut value and click **Apply** to save these changes.

Step 7 Select the **CFS** tab and select **commit** from the Config Action drop-down menu and click **Apply Changes** to distribute these changes to all switches in the fabric.

Verifying TACACS+ Configuration Using the CLI

To verify or change the TACACS+ configuration using the CLI, follow these steps:

Step 1 Use the **show tacacs-server** command to display configured TACACS+ parameters.

```
switch# show tacacs-server
Global TACACS+ shared secret:***********
timeout value:30
total number of servers:3

following TACACS+ servers are configured:
        11.5.4.3:
                available on port:2
        cisco.com:
                available on port:49
        11.6.5.4:
                available on port:49
                TACACS+ shared secret:*****
```

Step 2 Use the **tacacs-server host** *ip-address* **key** command to set the preshared key to match what is configured on your TACACS+ server.

Step 3 Use the **tacacs-server host** *ip-address* **port** command to set the communications port to match what is configured on your TACACS+ server.

Step 4 Use the **tacacs-server timeout** command to set the period in seconds for the switch to wait for a response from all TACACS+ servers before the switch declares a timeout failure.

Step 5 Use the **tacacs commit** command to commit any changes and distribute to all switches in the fabric.

Verifying RADIUS Server Monitor Configuration Using Fabric Manager

To verify or change the RADIUS server monitor configuration using Fabric Manager, follow these steps:

Step 1 Choose **Switches > Security > AAA > RADIUS** and select the **Servers** tab. You see the RADIUS configuration in the Information panel.

Step 2 Highlight the server that you need to change and click **Delete Row** to delete this server configuration.

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

Step 4 Set the KeyType and Key fields to the preshared key configured on the RADIUS server.

Step 5 Set the AuthPort and AcctPort fields to the authentication and accounting ports configured on the RADIUS server.

Step 6 Set the Idle Time to configure the time that the switch waits for a RADIUS server to be idle before sending a test message to see if the server is still alive.

Step 7 Set the TimeOut value and click **Apply** to save these changes.

Step 8 Select the **CFS** tab and select **commit** from the Config Action drop-down menu and click **Apply Changes** to distribute these changes to all switches in the fabric.

Step 9 Choose **Switches > Security > AAA a**nd click **Create Row** to create a server group.

Step 10 Check the list of switches that you want to configure server groups on.

Step 11 Set the Server List field to a comma-separated list of RADIUS servers.

Step 12 Set the Deadtime field to configure the time that the switch waits before retesting a dead server. and click **Apply** to save these changes.

Verifying RADIUS Server Monitor Configuration Using the CLI

To verify or change the RADIUS server monitor configuration using the CLI, follow these steps:

Step 1 Use the **show running-config** command to view the RADIUS configuration for the server monitor.

```
switch# show running-config | begin radius
radius-server deadtime 40
radius-server host 10.1.1.1 key 7 "VagwwtFjq" authentication accounting timeout 20
retransmit 5
radius-server host 10.1.1.1 test idle-time 30
```

Step 2 Use the **radius-server host** *ip address* **test idle-time** command to configure the time that the switch waits for a RADIUS server to be idle before sending a test message to see if the server is still alive.

Step 3 Use the **radius-server deadtime** command to configure the time that the switch waits before retesting a dead server.

Step 4 Use the **radius commit** command to commit any changes and distribute to all switches in the fabric.

Verifying TACACS+ Server Monitor Configuration Using Fabric Manager

To verify or change the TACACS+ server monitor configuration using Fabric Manager, follow these steps:

Step 1 Choose **Switches > Security > AAA > TACACS+** and select the **Servers** tab. You see the TACACS+ configuration in the Information panel.

Step 2 Highlight the server that you need to change and click **Delete Row** to delete this server configuration.

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

Step 4 Set the KeyType and Key fields to the preshared key configured on the TACACS+ server.

Step 5 Set the AuthPort and AcctPort fields to the authentication and accounting ports configured on the TACACS+ server.

Step 6 Set the Idle Time field to configure the time that the switch waits for a TACACS+ server to be idle before sending a test message to see if the server is still alive.

Step 7 Set the TimeOut value and click **Apply** to save these changes.

Step 8 Select the **CFS** tab and select **commit** from the Config Action drop-down menu and click **Apply Changes** to distribute these changes to all switches in the fabric.

Step 9 Choose **Switches > Security > AAA a**nd click **Create Row** to create a server group.

Step 10 Check the list of switches that you want to configure server groups on.

Step 11 Set the Server List field to a comma-separated list of TACACS+ servers.

Step 12 Set the Deadtime field to configure the time that the switch waits before retesting a dead server. and click **Apply** to save these changes.

Verifying TACACS+ Server Monitor Configuration Using the CLI

To verify or change the TACACS+ server monitor configuration using the CLI, follow these steps:

Step 1 Use the **show running-config** command to view the TACACS+ configuration for the server monitor.

```
switch# show running-config | begin tacacs
tacacs-server deadtime 40
tacacs-server host 11.6.5.4 key 7 "VagwwtFjq"
tacacs-server host 11.6.5.4 test idle-time 30
```

Step 2 Use the **tacacs-server host** *ip address* **test idle-time** command to configure the time that the switch waits for a TACACS+ server to be idle before sending a test message to see if the server is still alive.

Step 3 Use the **tacacs-server deadtime** command to configure the time that the switch waits before retesting a dead server.

Step 4 Use the **tacacs commit** command to commit any changes and distribute to all switches in the fabric.

User Authentication Fails

Symptom User authentication fails.

Table 17-2 User Authentication Fails

Symptom	Possible Cause	Solution
User authentication fails.	Incorrect AAA method configured.	Verify that the AAA method configured lists the appropriate RADIUS or TACACs+ server-group as the first one. For RADIUS servers, see the "Verifying RADIUS Configuration Using Fabric Manager" section on page 17-4 or the "Verifying RADIUS Configuration Using the CLI" section on page 17-4. For TACACS+ servers, see the "Verifying TACACS+ Configuration Using Fabric Manager" section on page 17-5 or the "Verifying TACACS+ Configuration Using the CLI" section on page 17-5.
	Incorrect authentication port configured or incorrect server timeout value.	Reconfigure the authentication port to match those configured on the AAA server or set a higher timeout value. For RADIUS servers, see the "Verifying RADIUS Configuration Using Fabric Manager" section on page 17-4 or the "Verifying RADIUS Configuration Using the CLI" section on page 17-4. For TACACS+ servers, see the "Verifying TACACS+ Configuration Using Fabric Manager" section on page 17-5 or the "Verifying TACACS+ Configuration Using the CLI" section on page 17-5.
	User not configured on the AAA server.	Add the user name, password, and role to the AAA server. Refer to your server documentation.
	AAA server not configured in the server group.	Add the appropriate AAA server to the configured server group. For RADIUS servers, see the "Verifying RADIUS Server Groups Using Fabric Manager" section on page 17-9 or the "Verifying RADIUS Server Groups Using the CLI" section on page 17-9. For TACACS+ servers, see the "Verifying TACACS+ Server Groups Using Fabric Manager" section on page 17-9 or the "Verifying TACACS+ Server Groups Using the CLI" section on page 17-10.

Verifying RADIUS Server Groups Using Fabric Manager

To verify or change the RADIUS server groups using Fabric Manager, follow these steps:

Step 1 Choose **Switches > Security > AAA a**nd click **Create Row** to create a server group.

Step 2 Check the list of switches that you want to configure server groups on.

Step 3 Set the Server List field to a comma-separated list of RADIUS servers.

Step 4 Set the Deadtime field to configure the time that the switch waits before retesting a dead server. and click **Apply** to save these changes.

Verifying RADIUS Server Groups Using the CLI

To verify or change the RADIUS server groups using the CLI, follow these steps:

Step 1 Use the **show running-config** command to view the RADIUS configuration for the server groups.

```
switch# show running-config | begin aaa
aaa group server radius RadiusGroup
    server 10.1.1.1
    server 10.2.3.4

aaa group server tacacs TacacsGroup
    server 11.5.4.3
    server 11.6.5.4
```

Step 2 Use the **aaa group server radius** command to configure the RADIUS servers that you want in this server group.

Note CFS does not distribute AAA server groups. You must copy this configuration to all relevant switches in the fabric.

Verifying TACACS+ Server Groups Using Fabric Manager

To verify or change the TACACS+ server groups using Fabric Manager, follow these steps:

Step 1 Choose **Switches > Security > AAA a**nd click **Create Row** to create a server group.

Step 2 Check the list of switches that you want to configure server groups on.

Step 3 Set the Server List field to a comma-separated list of TACACS+ servers.

Step 4 Set the Deadtime field to configure the time that the switch waits before retesting a dead server. and click **Apply** to save these changes.

Verifying TACACS+ Server Groups Using the CLI

To verify or change the TACACS+ server groups using the CLI, follow these steps:

Step 1 Use the **show running-config** command to view the TACACS+ configuration for the server groups.

```
switch# show running-config | begin aaa
aaa group server radius RadiusGroup
    server 10.1.1.1
    server 10.2.3.4

aaa group server tacacs TacacsGroup
    server 11.5.4.3
    server 11.6.5.4
```

Step 2 Use the **aaa group server tacacs** command to configure the TACACS+ servers that you want in this server group.

Note CFS does not distribute AAA server groups. You must copy this configuration to all relevant switches in the fabric.

User Is Not in Any Configured Role

Symptom User is not in any configured role.

Table 17-3 User Is Not In Any Configured Role

Symptom	Possible Cause	Solution

User is not in any configured role.	User configuration on AAA server does not have role attributes set.	For RADIUS, configure the vendor-specific attributes on the server for the role using:
		`Cisco-AVPair = shell:roles="rolename1 rolename2".`
		
		For TACACS+, configure the attribute and value pair on the server for the role using:
		`roles="rolename1 rolename2".`
		Verify that all roles are defined on the switch.

User Cannot Access Certain Features

Symptom User cannot access certain features.

Table 17-4 User Cannot Access Certain Features

Symptom	Possible Cause	Solution

User cannot access certain features.	User is assigned incorrect role.	For RADIUS, configure the vendor-specific attributes on the server for the role using:
		`Cisco-AVPair = shell:roles="rolename1 rolename2".`
		
		For TACACS+, configure the attribute/value pair on the server for the role using:
		`roles="rolename1 rolename2".`
		Verify that all roles are defined on the switch.

	Role is not configured for appropriate access.	See Chapter 18, "Troubleshooting Users and Roles."

Troubleshooting RADIUS and TACACS+ With Cisco ACS

To troubleshoot RADIUS and TACACS+ issues with Cisco ACS, follow these steps:

Step 1 Choose **Network Configuration** using Cisco ACS and view the AAA Clients table to verify that the Cisco SAN-OS switch is configured as an AAA client on Cisco ACS.

Step 2 Choose **User Setup > User Data Configuration** to verify that the user is configured.

Step 3 View the Cisco IOS/PIX RADIUS Attributes setting for a user. Verify that the user is assigned the correct roles in the AV-pairs. For example, `shell:roles="network-admin"`.

Note The Cisco IOS/PIX RADIUS Attributes field is case-sensitive. Verify that the role listed in the AV-pair exists on the Cisco SAN-OS switch.

Step 4 If the Cisco IOS/PIX RADIUS Attributes field is not present, follow these steps:

a. Choose **Interface > RADIUS (Cisco IOS/PIX).**

b. Check the **User** and **Group** check boxes for the cisco-av-pair option and click **Submit**.

c. Choose **User Setup > User Data Configuration** and add the AV-pair to assign the correct role to each user.

Step 5 Choose **System Configuration > Logging** to activate logs to look for reasons for failed authentication attempts.

Step 6 Choose **Reports and Activity** to view the resulting logs.

Step 7 On the Cisco SAN-OS switch, use the **show radius-server** command to verify that the RADIUS server timeout value is set to 5 seconds or greater.

Refer to the *User guide for Cisco Secure ACS* at the following website for more information:

http://cisco.com/en/US/products/sw/secursw/ps2086/products_user_guide_list.html