CHAPTER 4

Configuring AAA

This chapter describes how to configure authentication, authorization, and accounting (AAA) and includes the following sections:

Information About AAA

This section includes the following topics:

AAA Security Services

Based on a user ID and password combination, AAA is used to authenticate and authorize users. A key secures communication with AAA servers.

In many circumstances, AAA uses protocols such as RADIUS or TACACS+, to administer its security functions. If your router or access server is acting as a network access server, AAA is the means through which you establish communication between your network access server and your RADIUS or TACACS+, security server.

Although AAA is the primary (and recommended) method for access control, additional features for simple access control are available outside the scope of AAA, such as local username authentication, line password authentication, and enable password authentication. However, these features do not provide the same degree of access control that is possible by using AAA.

Separate AAA configurations are made for the following services:

- User Telnet or Secure Shell (SSH) login authentication
- Console login authentication
- User management session accounting

Table 4-1 shows the related CLI command for configuring an AAA service.

Table 4-1 AAA Service Configuration Commands

AAA Service Configuration Option	Related Command
Telnet or SSH login	**aaa authentication login default**
Console login	**aaa authentication login console**

AAA secures the following:

- Authentication, page 4-2
- Authorization, page 4-3
- Accounting, page 4-3

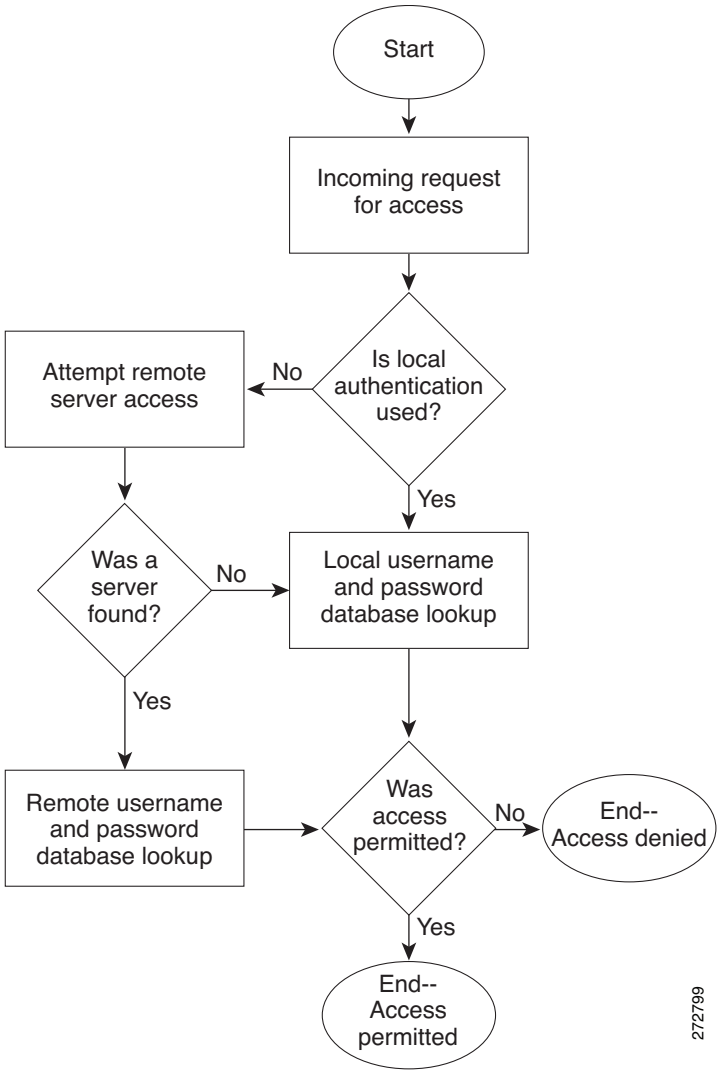
Authentication

Authentication identifies users with a login and password, messaging, and encryption.

Authentication is accomplished as follows:

Authentication Method	Description
Local database	Authenticates the following with a local lookup database of user names or passwords. • Console login authentication • User login authentication • User management session accounting
Remote RADIUS or TACACS+ server	Authenticates the following using a remote server lookup database of user names and passwords. • Console login authentication • User login authentication • User management session accounting
None	Authenticates the following with only a username. • Console login authentication • User login authentication • User management session accounting

Figure 4-1 Authenticating User Log In



Authorization

Authorization restricts the actions that a user is allowed to perform.

Accounting

Accounting tracks and maintains a log of every SVS management session. You can use this information to generate reports for troubleshooting and auditing purposes. You can store accounting logs locally or send them to remote AAA servers.

AAA Server Groups

Remote AAA server groups can provide fail-over in case one remote AAA server fails to respond. If the first server in the group fails, the next server in the group is tried until a server responds. Multiple server groups can provide fail-over for each other in this same way.

If all remote server groups fail, the local database is used for authentication.

Prerequisites for AAA

Authentication using remote AAA servers requires that the following be in place:

- At least one TACACS+ or RADIUS server is IP reachable
- The VSM is configured as an AAA server client.
- A shared secret key is configured on the VSM and the remote AAA server.

  See the "Configuring Shared Keys" procedure on page 6-9.

AAA Guidelines and Limitations

The Cisco Nexus 1000Vdoes not support user names made up of all numeric characters and does not create local user names made up of all numeric characters. If a username made up of all numeric characters exists on an AAA server and is entered during login, the Cisco Nexus 1000V does authenticate the user.

Default Settings

The following table lists the AAA defaults.

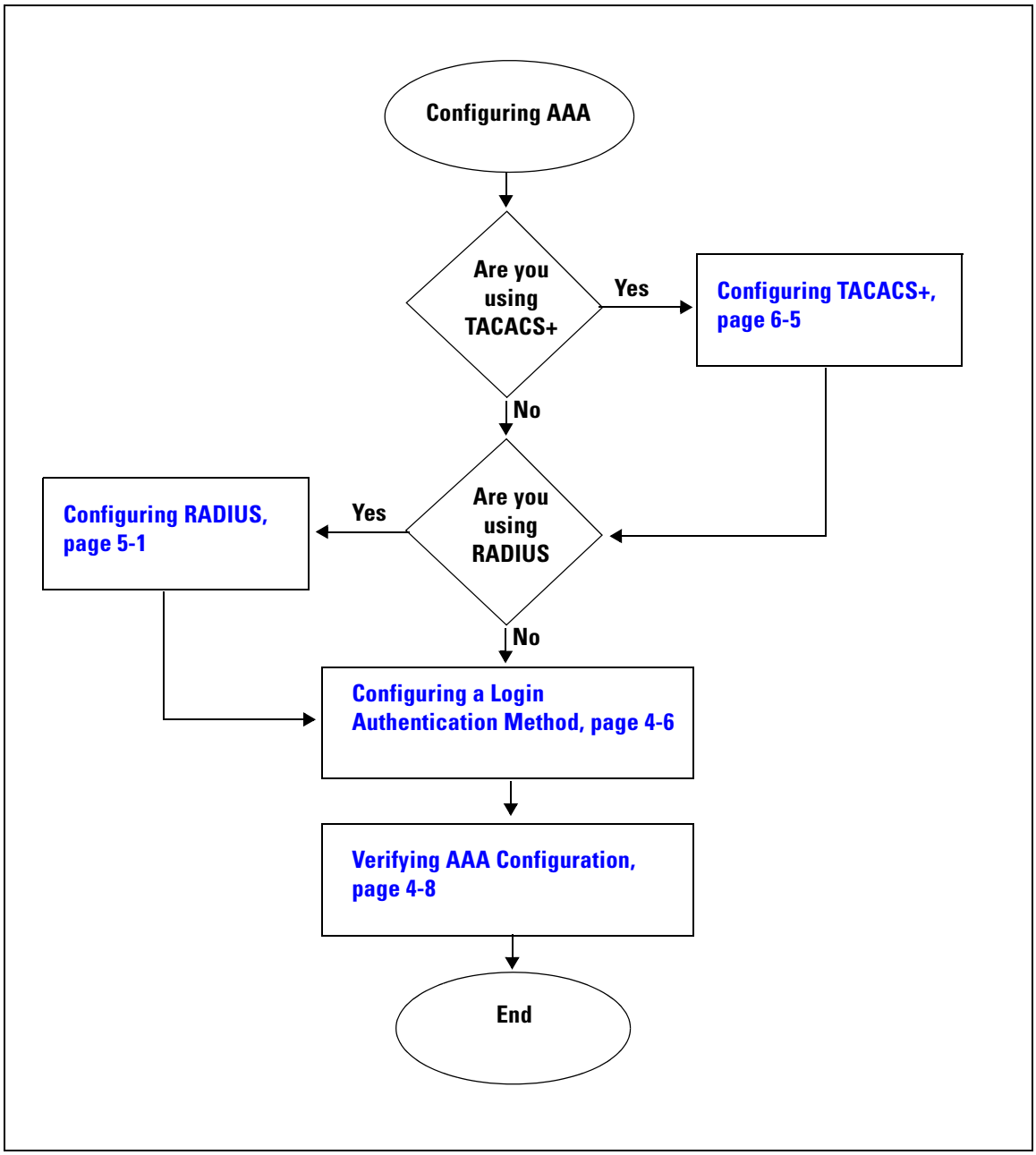
Parameters	Default
Console authentication method	**local**
Default authentication method	**local**
Login authentication failure messages	Disabled

Configuring AAA

This section includes the following topics:

Use the following flow chart to configure AAA.

Flow Chart: Configuring AAA



Configuring a Login Authentication Method

Use this procedure to configure the login authentication method.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- If authentication is to be done with TACACS+ server group(s), you have already added the group(s). For more information, see Configuring a TACACS+ Server Group, page 6-12.

SUMMARY STEPS

1. **config t**
2. **aaa authentication login {console | default}** {**group** *group-list* [**none**] | **local** | **none**}
3. **exit**
4. **show aaa authentication**
5. **copy running-config start-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into the CLI Global Configuration mode.

Step 2	**aaa authentication login {console | default}** {**group** *group-list* [**none**]| **local** | **none**} **Example:** `n1000v(config)# aaa authentication login console group tacgroup`	Configures the console or default login authentication method. • **group**: Authentication is done by server group(s). – **group-list**: List server group names separated by spaces; or none for no authentication. • **local:** The local database is used for authentication. **Note** Local is the default and is used when no methods are configured or when all the configured methods fail to respond. • **none:** Authentication is done by username.

Step 3	**exit**
	
	Example:
	`n1000v(config)# exit`
	`n1000v#`
		Exits the CLI Global Configuration mode and returns you to EXEC mode.

	Command	Purpose

Step 4	**show aaa authentication**
	
	Example:
	`n1000v# show aaa authentication`
	`default: group tacgroup`
	`console: group tacgroup`
	`n1000v#`
		(Optional) Displays the configured login authentication method.

Step 5	**copy running-config startup-config** **Example:** `n1000v# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Enabling Login Authentication Failure Messages

Use this procedure to enable the login authentication failure message to displays if the remote AAA servers do not respond.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- The following is the Login Authentication Failure message:

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

SUMMARY STEPS

1. **config t**
2. **aaa authentication login error-enable**
3. **exit**
4. **show aaa authentication login error-enable**
5. **copy running-config start-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you in CLI Global Configuration mode.

Step 2	**aaa authentication login error-enable**
	
	Example:
	`n1000v(config)# aaa authentication login error-enable`
	`n1000v(config)#`
		Enables login authentication failure messages. The default is disabled.

	Command	Purpose

Step 3	**exit**
	
	Example:
	`n1000v(config)# exit`
	`n1000v#`
		Exits CLI Global Configuration mode and returns you to EXEC mode.

Step 4	**show aaa authentication login error-enable**
	
	Example:
	
	`n1000v# show aaa authentication login error-enable`
	`enabled`
	`n1000v#`
		(Optional) Displays the login failure message configuration.

Step 5	**copy running-config startup-config** **Example:** `n1000v# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Verifying AAA Configuration

To display AAA configuration information, perform one of the following tasks:

Command	Purpose
show aaa authentication [**login** {**error-enable** | **mschap**}]	Displays AAA authentication information. See Example 4-1 on page 4-8
show aaa groups	Displays the AAA server group configuration.
show running-config aaa [**all**]	Displays the AAA configuration in the running configuration. See Example 4-2 on page 4-8
show startup-config aaa	Displays the AAA configuration in the startup configuration. See Example 4-3 on page 4-9

Example 4-1 show aaa authentication

```
n1000v# show aaa authentication login error-enable
disabled
```

Example 4-2 show running config aaa

```
n1000v# show running-config aaa all
version 4.0(1)
aaa authentication login default local
aaa accounting default local
no aaa authentication login error-enable
no aaa authentication login mschap enable
no radius-server directed-request
no snmp-server enable traps aaa server-state-change
```

```
no tacacs-server directed-request
n1000v#
```

Example 4-3 show startup-config aaa

```
n1000v# show startup-config aaa
version 4.0(1)svs#
```

Example AAA Configuration

The following is an AAA configuration example:

```
aaa authentication login default group tacacs
aaa authentication login console group tacacs
```

Additional References

For additional information related to implementing AAA, see the following sections:

- Related Documents, page 4-9
- Standards, page 4-9

Related Documents

Related Topic	Document Title
System Management	*Cisco Nexus 1000V System Management Configuration Guide, Release 4.2(1)SV1(4)*
CLI	*Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(4)*
TACACS+ Security protocol	Chapter 6, “Configuring TACACS+”

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for AAA

This section provides the AAA release history.

Feature Name	Releases	Feature Information
AAA	4.0(4)SV1(1)	This feature was introduced.