CHAPTER 7

Configuring the Network Access Server

Configuring the CiscoSecure server is only half of the configuration tasks required for an operational system. The other half of configuration tasks is configuring the network access server so that is functions properly with the CiscoSecure server.

This chapter describes how to configure the network access server and contains the following sections:

- Global Configuration
- Authentication on the Network Access Server
- Authorization on the Network Access Server
- Accounting on the Network Access Server
- Other Commands

For complete information about a specific Cisco IOS release or more detailed configurations, refer to the publication *Router Products Configuration Guide* or the *Configuration Fundamentals Configuration Guide*. (See the appendix “References and Recommended Reading”)

Global Configuration

The first steps in configuring the network access server are to enable TACACS+, specify the list of CiscoSecure servers that will provide AAA services for the network access server, and configure the encryption key that is used to encrypt the data transfer between the network access server and the CiscoSecure server.

To begin global configuratin, enter the following commands, using the correct IP address of the CiscoSecure servers and your own encryption key:

```
Router(config)#aaa new-model
Router(config)#tacacs-server host 144.1.12.100
Router(config)#tacacs-server host 144.1.200.250
Router(config)#tacacs-server key arachnid
```

The word arachnid is the encryption key that is shared between the network access server and the CiscoSecure server. The encryption key should be kept secret in order to protect the privacy of passwords that are sent between the CiscoSecure server and the network access server during the authentication process.

You can specify multiple CiscoSecure servers by repeating the **tacacs-server host** command.

Authentication on the Network Access Server

The authentication configuration builds a set of authentication lists, each of which can be used for different purposes within the network access server. The syntax of the command is as follows:

aaa authentication login *list_name method1 [method2] [method3] [method4]*

Each of the authentication methods is listed in Table 7-1:

Table 7-1 Network Access Server Authentication Methods

Method	Meaning
enable	Use the enable password.
line	Use the line password.
local	Use the network access server internal username database.
none	Use no authentication.
tacacs+	Use TACACS+ authentication.

In the following example, system administrators must use TACACS+ authentication and, if a CiscoSecure server is not available, fall back to using the router enable password. However, all other users must use only TACACS+:

```
aaa authentication default tacacs+
aaa authentication admin tacacs+ enable
```

To configure authentication at login on all lines on a 16-port network access server, enter the following commands:

```
line console 0
login authentication admin
line aux 0
login authentication admin
line vty 0 4
login authentication default
line 1 16
login authentication default
```

Note If you do not include the enable method for system administrator logins, you will no longer be able to login to your network access server unless you have a functioning CiscoSecure server appropriately configured with usernames and passwords. The addition of the enable method ensures that you will still be able to log in to the router if the router cannot contact a CiscoSecure server. Only if the network access server cannot contact a CiscoSecure server will it test the enable method.

Excluding Ports

Network access server ports may be excluded from using CiscoSecure by creating a separate authentication method list which does not include TACACS+ as an authentication method. Depending on your needs, you create a separate authentication method list to fixed ports that do not need AAA services, or for all the vty ports.

In the following example, only the first two vty ports and the console are enabled for AAA services in the network access server configuration:

```
aaa new-model
aaa authentication login admin tacacs+ enable
aaa authentication login no_tacacs line
tacacs-server host 144.251.1.1
```

```
tacacs-server key arachnid
! The console and VTY lines 0 & 1 use TACACS+
line console 0
login authentication admin
line vty 0 1
login authentication admin
! VTY Lines 2 - 4 do not use TACACS+
line vty 2 4
login authentication no_tacacs
```

Authorization on the Network Access Server

The network access server can use a CiscoSecure server to authorize specific commands by individual users. To authorize specific commands, you must specify which commands and actions will require authorization checks, using the following command syntax:

aaa authorization {network | connection | exec | commands *level***}** *methods*

The four items that can be checked for authorization are listed in Table 7-2.

Table 7-2 Checkable Authorization Items on the Network Access Server

Keyword	Authorization Check
network	Check authorization for all network activities including SLIP, PPP, PPP network control protocols, and ARAP.
connection	Check authorization for outbound telnet and rlogin.
exec	Determine if the user is allowed to run an EXEC shell when logging into the network access server. This keyword may cause CiscoSecure UNIX server to return user profile information such as autocommand information.
commands *level*	Check authorization for all commands at the specified privilege level *level*. Valid levels are 0 through 15. Level 1 is normal user EXEC commands. Level 15 is normal privileged level.

The *methods* you can specify are listed in Table 7-3.

Table 7-3 Authorization Methods on the Network Access Server

Method	Meaning
tacacs+	Requests authorization information from the CiscoSecure server.
if-authenticated	Allows the user to access the requested function if the user is authenticated. Note that you are either authenticated or not, so this should be the last method in the list.
none	No authorization is performed.
local	Uses the local database for authorization.

Using the command syntax specified above, you can configure the network access server to restrict the set of commands that an individual user can execute. To require that all commands at privilege level 1 be authorized, enter the following command:

```
aaa authorization commands 1 tacacs+
```

Note When you enter this command in your network access server, you will be permitted to execute only network access server commands that are allowed by your CiscoSecure server. Therefore, you should ensure that you have configured, on CiscoSecure, an authenticated user who is authorized to run commands.

To require that the system administrators be authorized at level 15, enter the following command:

```
aaa authorization commands 15 tacacs+ if-authenticated
```

This command uses TACACS+ authorization level 15 but if problems arise you can switch off the CiscoSecure server and the authorization will then be granted to anyone who is authenticated.

Note The network access server will test the *if-authenticated* method only if it cannot contact a CiscoSecure server.

Accounting on the Network Access Server

The network access server must be specifically configured to send accounting records to the CiscoSecure server. Several types of accounting records are available. Use the following command syntax to configure accounting on the network access server:

```
aaa accounting {system | network | connection | exec | command level}
{start-stop | wait-start | stop-only} tacacs+
```

The first set of keywords allows you to specify accounting of the events listed in Table 7-4.

Table 7-4 Accounting Events on the Network Access Server

Event Type	Meaning
system	Enables accounting for all system-level events not associated with users, such as reloads.
network	Enables accounting for all network-related requests, including SLIP, PPP, PPP network control protocols, and ARA protocol
connection	Enables accounting for outbound Telnet and rlogin.
exec	Enables accounting for EXEC processes (user shells).
command *level*	Enables accounting for all commands at the specified privilege level, 0 through 15.

You can specify when accounting records are to be sent by using the second set of keywords, which are listed in Table 7-5.

Table 7-5 Accounting Record Keywords on the Network Access Server

Keyword	Meaning
stop-only	The network access server sends a stop record accounting notice at the end of the specified activity or event (command, EXEC shell, etc.)
start-stop	The network access server sends a start record accounting notice at the beginning of a process and a stop record at the end of the process. The start accounting record is sent in the background. The requested user process begins regardless of whether or not the start accounting record was acknowledged by the accounting server.
wait-start	Causes both a start and stop accounting record to be sent to the accounting server. However, the requested user service does not begin until the start accounting record is acknowledged. A stop accounting record is also sent.

Use the following commands to record accounting information on network access server system events, network connections, outbound connections, EXEC operations, and commands at level 1 and level 15:

```
aaa accounting system start-stop tacacs+
aaa accounting network start-stop tacacs+
aaa accounting connection start-stop tacacs+
aaa accounting exec stop-only tacacs+
aaa accounting command 1 stop-only tacacs+
aaa accounting command 15 wait-start tacacs+
```

Note **Stop** records contain elapsed time for connections and EXEC sessions.

Note The command, aaa accounting command 0 start-stop, is not implemented in Cisco IOS release 11.0. Check the release notes for your Cisco IOS release to determine whether it has been implemented.

Other Commands

You can use other commands to tailor the operation of the network access server with the TACACS+ protocol. Refer to the publications *Router Products Command Reference* or *Configuration Fundamentals Command Reference* for a detailed list of commands. (See the appendix, “References and Recommended Reading.”