

Configuring the NAS for RADIUS

Configuration for the network access server (NAS) using the Remote Access Dial-In User Service (RADIUS) protocol is similar to configuration for the Terminal Access Controller Access Control System (TACACS+) protocol.

This chapter describes:

- Global Configuration
- Authentication on the NAS
- Authorization on the NAS
- Accounting on the NAS
- Sample Configuration for a Cisco 2509 Using RADIUS with Accounting Enabled
- Sample Configuration for an ISP Using a Cisco AS5200

Note The information in this chapter applies to Cisco NASes; however, you can use the CiscoSecure Access Control Server (ACS) with other vendors' NASes. See your manufacturer's documentation for more specific information on configuring your NAS. Configure your NAS for RADIUS as you would normally; no special configuration is required.

For complete information about a specific Cisco IOS release or more detailed configurations, see the *Router Products Configuration Guide* or the *Configuration Fundamentals Configuration Guide* publication. (See Appendix A, "References and Recommended Reading.")

Note For a sample configuration, see the “Sample Configuration for a Cisco 2509 Using RADIUS with Accounting Enabled” section on page 10-9 and the “Sample Configuration for an ISP Using a Cisco AS5200” section on page 10-12. For more ready-to-use configurations, see the chapter “NAS Configuration Examples,” in the *CiscoSecure ACS 2.3 for UNIX Reference Guide* for sample configurations that you can apply directly to your own NAS or modify according to your needs.

Global Configuration

The first steps in configuring the NAS are:

- 1 Enable RADIUS.
- 2 Specify the list of CiscoSecure ACSs that will provide AAA services for the NAS.
- 3 Configure the encryption key that is used to encrypt the data transfer between the NAS and the CiscoSecure ACS.

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

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

The word “arachnid” is the encryption key shared between the NAS and the CiscoSecure ACS. The encryption key should be kept secret to protect the privacy of passwords sent between the CiscoSecure ACS and the NAS during the authentication process.

For backup purposes, you can specify multiple CiscoSecure ACSes by repeating the **radius-server host** command.

For a RADIUS-enabled NAS to use a CiscoSecure ACS, it must be added to the list of available RADIUS-enabled NASes in the NASes page of that ACS’s the Java-based CiscoSecure Administrator advanced configuration program.

Authentication on the NAS

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

```
aaa authentication login list_name method1 [method2] [method3] [method4]
aaa authentication PPP list_name method1 [method2] [method3] [method4]
```

As you can see, the AAA server requires an authentication for PPP in addition to an authentication for login before it will work properly.

Each of these command lines supports several arguments. A list name and one authentication method are required. Additional authentication methods are optional.

Each of the authentication methods is listed in Table 10-1.

Table 10-1 **NAS Authentication Methods**

Method	Meaning
enable	Use the enable password.
line	Use the line password.
local	Use the NAS internal username database.
none	Use no authentication.
RADIUS	Use RADIUS authentication.

In the following example, system administrators must use RADIUS authentication. If a CiscoSecure ACS is not available, use the NAS's local user database password. However, all other users must use only RADIUS:

```
aaa authentication login default radius
aaa authentication login admin radius local
```

Excluding Ports

To configure authentication at login on all lines on a 16-port NAS, 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
```



Caution If you do not include the enable method for system administrator logins, you will no longer be able to log in to your NAS unless you have a functioning CiscoSecure ACS 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 ACS. The NAS will test the enable method only if it cannot contact a CiscoSecure ACS.

Excluding Ports

NAS ports can be excluded from using the CiscoSecure ACS by creating a separate authentication method list that does not include RADIUS as an authentication method. Depending on your needs, you create a separate authentication method list to fixed ports that do not need authentication, authorization, and accounting (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 NAS configuration:

```
aaa new-model
aaa authentication login admin radius local
aaa authentication login no_radius line
radius-server host 144.251.1.1
radius-server key arachnid
! The console and VTY lines 0 & 1 use RADIUS
line console 0
login authentication admin
line vty 0 1
login authentication admin
! VTY Lines 2 - 4 do not use RADIUS
line vty 2 4
login authentication no_radius
```

Authorization on the NAS

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

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

The four items that can be checked for authorization are listed in Table 10-2.

Table 10-2 Checkable Authorization Items on the NAS

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 NAS. This keyword might cause the CiscoSecure ACS to return user profile information such as autocommand information.

Authorization on the NAS

Table 10-2 Checkable Authorization Items on the NAS (continued)

commands <i>level</i>	Check authorization for all commands at the specified privilege level <i>level</i> . Valid levels are 1 through 15. Level 1 is normal user EXEC commands. Level 15 is normal privileged level.
-----------------------	--

The methods you can specify are listed in Table 10-3.

Table 10-3 Authorization Methods on the NAS

Method	Meaning
radius	Requests authorization information from the CiscoSecure ACS.
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 NAS to restrict the set of commands that an individual user can execute. To require that all commands entered by users at privilege level 1 be checked for ACS authorization, enter the following command:

```
aaa authorization commands 1 radius
```



Caution When you enter this command in your NAS, you will be permitted to execute only NAS commands that are allowed by your CiscoSecure ACS. Therefore, make sure you have configured an authenticated user who is authorized to run commands on the CiscoSecure ACS.

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

```
aaa authorization commands 15 radius if-authenticated
```

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

Note The NAS will test the if-authenticated method only if it cannot contact a CiscoSecure ACS.

Accounting on the NAS

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

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

The first set of keywords allows you to specify accounting of the events listed in Table 10-4.

Table 10-4 **Accounting Events on the NAS**

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 ARAP
connection	Enables accounting for outbound Telnet and rlogin
exec	Enables accounting for EXEC processes (user shells)
command <i>level</i>	Enables accounting for all commands at the specified privilege level

You can specify when accounting records are to be sent by using the second set of keywords, which are listed in Table 10-5.

Accounting on the NAS

Table 10-5 Accounting Record Keywords on the NAS

Keyword	Meaning
stop-only	The NAS sends a stop record accounting notice at the end of the specified activity or event (command, EXEC shell, and so on).
start-stop	The NAS 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	This keyword 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 NAS system events, network connections, outbound connections, EXEC operations, and commands at level 1 and level 15:

```
aaa accounting system start-stop radius
aaa accounting network start-stop radius
aaa accounting connection start-stop radius
aaa accounting exec stop-only radius
aaa accounting command 1 stop-only radius
aaa accounting command 15 wait-start radius
Stop records contain elapsed time for connections and EXEC sessions.
```

Note The **aaa accounting command 0 start-stop** command 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.

Sample Configuration for a Cisco 2509 Using RADIUS with Accounting Enabled

The following is a sample configuration for a Cisco 2509 router using RADIUS with the accounting feature enabled:

```
Current configuration:
!
version 11.2
service udp-small-servers
service tcp-small-servers
!
hostname as2509
!
aaa new-model
aaa authentication local-override
aaa authentication login default radius
aaa authentication login no_radius local
aaa authentication enable default enable
aaa authentication ppp default radius
aaa authorization exec radius if-authenticated
aaa authorization network radius
aaa accounting exec start-stop radius
aaa accounting network start-stop radius
aaa accounting system start-stop radius
enable password secure
!
username cisco password 7 03175E08131D24
username therzog password 7 09404B1D14001E1C59
username root password 7 070C285F4D06
ip address-pool local
chat-script cisco-default ABORT ERROR "" "AT Z" OK "ATDT \T" TIMEOUT 30
\c CONNECT \c
chat-script usr-courier-veverything "" "AT&FS0=1&C1&D2&H1&R2&N14&B1&W"
chat-script factory-default "" "AT&F"
!
interface Ethernet0
ip address 200.200.200.44 255.255.255.0
no mop enabled
!
interface Serial0
no ip address
shutdown
!
```

Sample Configuration for a Cisco 2509 Using RADIUS with Accounting Enabled

```
interface Serial1
no ip address
shutdown
!
interface Async1
ip unnumbered Ethernet0
encapsulation ppp
sync mode interactive
peer default ip address 200.200.200.58
no cdp enable
ppp authentication chap pap
!
interface Async2
ip unnumbered Ethernet0
encapsulation ppp
async mode interactive
peer default ip address pool pool1
no cdp enable
ppp authentication pap chap
!
interface Group-Async1
ip unnumbered Ethernet0
encapsulation ppp
no cdp enable
group-range 3 8
!
ip local pool pool1 200.200.200.50 200.200.200.57
no ip classless
!
radius-server host 200.200.200.41
radius-server key as2509abcd
!
line con 0
session-timeout 10
exec-timeout 30 0
login authentication no_radius
transport preferred none
line 1
autoselect during-login
autoselect ppp
script startup usr-courier-veverything
script reset usr-courier-veverything
modem InOut
modem autoconfigure type usr_courier
transport input all
```

Sample Configuration for a Cisco 2509 Using RADIUS with Accounting Enabled

```
rxspeed 115200
txspeed 115200
flowcontrol hardware
line 2
autoselect ppp
script startup usr-courier-veverything
script reset usr-courier-veverything
modem InOut
modem autoconfigure type usr_courier
transport input all
rxspeed 115200
txspeed 115200
flowcontrol hardware
line 3 8
transport input all
rxspeed 115200
txspeed 115200
flowcontrol hardware
line aux 0
transport preferred none
transport input all
line vty 0
exec-timeout 0 0
width 102
transport preferred none
line vty 1
exec-timeout 0 0
length 35
width 127
transport preferred none
line vty 2 4
exec-timeout 0 0
transport preferred none
!
end
as2509#
```

Sample Configuration for an ISP Using a Cisco AS5200

The following sample configuration for a Cisco AS5200 is typical of one that can be used by an Internet service provider (ISP) with a RADIUS installation. This configuration includes AAA, allowing the ISP to have centralized user management as well as accounting records necessary for billing:

```
!  
version 11.1  
service udp-small-servers  
service tcp-small-servers  
!  
hostname isdn-14  
!  
aaa new-model  
aaa authentication login default Radius  
aaa authentication login console line  
aaa authentication login secure radius local  
aaa authentication login vty line  
aaa authentication ppp default Radius  
aaa authentication ppp secure if-needed radius local  
aaa authorization exec radius  
aaa authorization network radius  
aaa accounting exec start-stop radius  
aaa accounting network start-stop radius  
!  
username backup password radiusISdown  
ip radius source-interface Ethernet0  
rlogin trusted-remoteuser-source local  
rlogin trusted-localuser-source radius  
isdn switch-type primary-5ess  
!  
controller T1 0  
framing esf  
clock source line primary  
linecode b8zs  
pri-group timeslots 1-24  
!  
controller T1 1  
framing esf  
clock source line secondary  
linecode b8zs  
pri-group timeslots 1-24
```

Sample Configuration for an ISP Using a Cisco AS5200

```
!  
interface Loopback0  
ip address 171.68.187.254 255.255.255.0  
!  
interface Ethernet0  
ip address 172.16.25.15 255.255.255.224  
!  
interface Serial0  
no ip address  
shutdown  
!  
interface Serial1  
no ip address  
shutdown  
!  
interface Serial0:23  
ip unnumbered Loopback0  
encapsulation ppp  
isdn incoming-voice modem  
peer default ip address pool default  
dialer rotary-group 1  
dialer-group 1  
!  
interface Serial1:23  
ip unnumbered Loopback0  
encapsulation ppp  
isdn incoming-voice modem  
peer default ip address pool default  
dialer rotary-group 1  
dialer-group 1  
!  
interface Group-Async1  
ip unnumbered Loopback0  
ip tcp header-compression passive  
encapsulation ppp  
async mode interactive  
peer default ip address pool default  
dialer-group 1  
ppp authentication chap pap secure  
group-range 1 48  
!  
interface Dialer1  
ip unnumbered Loopback0  
encapsulation ppp  
peer default ip address pool default
```

Sample Configuration for an ISP Using a Cisco AS5200

```
ppp multilink
ppp authentication chap pap secure
dialer-group 1
!
ip local pool default 171.68.187.1 171.68.187.48
ip domain-name cisco.com
ip name-server 171.68.10.70
no ip classless
async-bootp dns-server 171.68.10.70
!
radius-server host 172.16.72.41
radius-server host 172.16.72.42
radius-server timeout 3
radius-server key MYSECRET
!
dialer-list 1 protocol ip permit
!
line con 0
login authentication console
password cisco
line 1 48
session-timeout 15 output
autoselect during-login
autoselect ppp
login authentication secure
modem InOut
transport input all
line aux 0
line vty 0 4
login authentication vty
password secret
!
end
```