Configuring RADIUS

This chapter describes the Remote Authentication Dial-In User Service (RADIUS) security system, defines its operation, and identifies appropriate and inappropriate network environments for using RADIUS technology. The “RADIUS Configuration Task List” section describes how to configure RADIUS with the authentication, authorization, and accounting (AAA) command set. The “RADIUS Authentication and Authorization Example” section at the end of this chapter offers two possible implementation scenarios.

This section includes the following topics:

- RADIUS Overview
- RADIUS Operation
- RADIUS Configuration Task List

For a complete description of the commands used in this chapter, refer to the “RADIUS Commands” chapter in the *Security Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

RADIUS Overview

RADIUS is a distributed client/server system that secures networks against unauthorized access. In the Cisco implementation, RADIUS clients run on Cisco routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information.

RADIUS is a fully open protocol, distributed in source code format, that can be modified to work with any security system currently available on the market.

Cisco supports RADIUS under its AAA security paradigm. RADIUS can be used with other AAA security protocols, such as TACACS+, Kerberos, or local username lookup. RADIUS is supported on all Cisco platforms.

RADIUS has been implemented in a variety of network environments that require high levels of security while maintaining network access for remote users.

Use RADIUS in the following network environments that require access security:

- Networks with multiple-vendor access servers, each supporting RADIUS. For example, access servers from several vendors use a single RADIUS server-based security database. In an IP-based network with multiple vendors’ access servers, dial-in users are authenticated through a RADIUS server that has been customized to work with the Kerberos security system.

- Turnkey network security environments in which applications support the RADIUS protocol, such as in an access environment that uses a “smart card” access control system. In one case, RADIUS has been used with Enigma’s security cards to validate users and grant access to network resources.
- Networks already using RADIUS. You can add a Cisco router with RADIUS to the network. This might be the first step when you make a transition to a Terminal Access Controller Access Control System (TACACS+) server.
- Networks in which a user must only access a single service. Using RADIUS, you can control user access to a single host, to a single utility such as Telnet, or to a single protocol such as Point-to-Point Protocol (PPP). For example, when a user logs in, RADIUS identifies this user as having authorization to run PPP using IP address 10.2.3.4 and the defined access list is started.
- Networks that require resource accounting. You can use RADIUS accounting independent of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, indicating the amount of resources (such as time, packets, bytes, and so on) used during the session. An Internet service provider (ISP) might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.

RADIUS is not suitable in the following network security situations:

- Multiprotocol access environments. RADIUS does not support the following protocols:
  - AppleTalk Remote Access Protocol (ARAP)
  - NetBIOS Frame Protocol Control Protocol (NBFCP)
  - NetWare Asynchronous Services Interface (NASI)
  - X.25 PAD connections
- Router-to-router situations. RADIUS does not provide two-way authentication. RADIUS can be used to authenticate from one router to a non-Cisco router if the non-Cisco router requires RADIUS authentication.
- Networks using a variety of services. RADIUS generally binds a user to one service model.

RADIUS Operation

When a user attempts to log in and authenticate to an access server using RADIUS, the following steps occur:

1. The user is prompted for and enters a username and password.
2. The username and encrypted password are sent over the network to the RADIUS server.
3. The user receives one of the following responses from the RADIUS server:
   - ACCEPT—The user is authenticated.
   - REJECT—The user is not authenticated and is prompted to reenter the username and password, or access is denied.
   - CHALLENGE—A challenge is issued by the RADIUS server. The challenge collects additional data from the user.
   - CHANGE PASSWORD—A request is issued by the RADIUS server, asking the user to select a new password.

The ACCEPT or REJECT response is bundled with additional data that is used for EXEC or network authorization. You must first complete RADIUS authentication before using RADIUS authorization. The additional data included with the ACCEPT or REJECT packets consists of the following:

- Services that the user can access, including Telnet, rlogin, or local-area transport (LAT) connections, and PPP, Serial Line Internet Protocol (SLIP), or EXEC services.
- Connection parameters, including the host or client IP address, access list, and user timeouts.

RADIUS Configuration Task List

To configure RADIUS on your Cisco router or access server, you must perform the following tasks:

- Use the **aaa new-model** global configuration command to enable AAA. AAA must be configured if you plan to use RADIUS. For more information about using the **aaa new-model** command, refer to the "AAA Overview" chapter.
- Use the **aaa authentication** global configuration command to define method lists for RADIUS authentication. For more information about using the **aaa authentication** command, refer to the "Configuring Authentication" chapter.
- Use **line** and **interface** commands to enable the defined method lists to be used. For more information, refer to the "Configuring Authentication" chapter.

The following configuration tasks are optional:

- If needed, use the **aaa authorization** global command to authorize specific user functions. For more information about using the **aaa authorization** command, refer to the "Configuring Authorization" chapter.
- If needed, use the **aaa accounting** command to enable accounting for RADIUS connections. For more information about using the **aaa accounting** command, refer to the "Configuring Accounting" chapter.

This section describes how to set up RADIUS for authentication, authorization, and accounting on your network, and includes the following sections:

- Configure Router to RADIUS Server Communication
- Configure Router to Use Vendor-Specific RADIUS Attributes
- Configure Router for Vendor-Proprietary RADIUS Server Communication
- Configure Router to Query RADIUS Server for Static Routes and IP Addresses
- Configure Router to Expand Network Access Server Port Information
- Configure Router to Expand Network Access Server Port Information
- Specify RADIUS Authorization
- Specify RADIUS Accounting

Configure Router to RADIUS Server Communication

The RADIUS host is normally a multiuser system running RADIUS server software from Livingston, Merit, Microsoft, or another software provider. A RADIUS server and a Cisco router use a shared secret text string to encrypt passwords and exchange responses.

To configure RADIUS to use the AAA security commands, you must specify the host running the RADIUS server daemon and a secret text string that it shares with the router. Use the **radius-server** commands to specify the RADIUS server host and a secret text string.

To specify a RADIUS server host and shared secret text string, perform the following tasks in global configuration mode:

Task	Command
Specify the IP address or host name of the remote RADIUS server host and assign authentication and accounting destination port numbers.	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*]
Specify the shared secret text string used between the router and the RADIUS server.	**radius-server key** *string*

To customize communication between the router and the RADIUS server, use the following optional **radius-server** global configuration commands:

Task	Command
Specify the number of times the router transmits each RADIUS request to the server before giving up (default is three).	**radius-server retransmit** *retries*
Specify the number of seconds a router waits for a reply to a RADIUS request before retransmitting the request.	**radius-server timeout** *seconds*
Specify the number of minutes a RADIUS server, which is not responding to authentication requests, is passed over by requests for RADIUS authentication.	**radius-server deadtime** *minutes*

Configure Router to Use Vendor-Specific RADIUS Attributes

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

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

“Protocol” is a value of the Cisco “protocol” attribute for a particular type of authorization. “Attribute” and “value” are an appropriate attribute/value (AV) pair defined in the Cisco TACACS+ specification, and “sep” is “=” for mandatory attributes and “*” for optional attributes. This allows the full set of features available for TACACS+ authorization to also be used for RADIUS.

For example, the following AV pair causes Cisco’s “multiple named ip address pools” feature to be activated during IP authorization (during PPP’s IPCP address assignment):

```
cisco-avpair= ”ip:addr-pool=first“
```

The following example causes a “NAS Prompt” user to have immediate access to EXEC commands.

```
cisco-avpair= ”shell:priv-lvl=15“
```

Other vendors have their own unique vendor-IDs, options, and associated VSAs. For more information about vendor-IDs and VSAs, refer to RFC 2138, "Remote Authentication Dial-In User Service (RADIUS)."

To configure the NAS to recognize and use VSAs, perform the following task in global configuration mode:

Task	Command
Enable the network access server to recognize and use VSAs as defined by RADIUS IETF attribute 26.	**radius-server vsa send [accounting | authentication]**

For a complete list of RADIUS attributes or more information about vendor-specific Attribute 26, refer to the RADIUS Attributes appendix.

Configure Router for Vendor-Proprietary RADIUS Server Communication

Although the IETF draft standard for RADIUS specifies a method for communicating vendor-specific information between the network access server and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. Cisco IOS software supports a subset of vendor-proprietary RADIUS attributes.

As mentioned earlier, to configure RADIUS (whether vendor-proprietary or IETF draft-compliant), you must specify the host running the RADIUS server daemon and the secret text string it shares with the Cisco device. You specify the RADIUS host and secret text string by using the **radius-server** commands. To identify that the RADIUS server is using a vendor-proprietary implementation of RADIUS, use the **radius-server host non-standard** command. Vendor-proprietary attributes will not be supported unless you use the **radius-server host non-standard** command.

To specify a vendor-proprietary RADIUS server host and a shared secret text string, perform the following tasks in global configuration mode:

Task	Command
Specify the IP address or host name of the remote RADIUS server host and identify that it is using a vendor-proprietary implementation of RADIUS.	**radius-server host** {*hostname* | *ip-address*} **non-standard**
Specify the shared secret text string used between the router and the vendor-proprietary RADIUS server. The router and the RADIUS server use this text string to encrypt passwords and exchange responses.	**radius-server key** *string*

Configure Router to Query RADIUS Server for Static Routes and IP Addresses

Some vendor-proprietary implementations of RADIUS let the user define static routes and IP pool definitions on the RADIUS server instead of on each individual network access server in the network. Each network access server then queries the RADIUS server for static route and IP pool information.

To have the Cisco router or access server query the RADIUS server for static routes and IP pool definitions when the device first starts up, perform the following task in global configuration mode:

Task	Command
Tell the Cisco router or access server to query the RADIUS server for the static routes and IP pool definitions used throughout its domain.	**radius-server configure-nas**

Note Because the **radius-server configure-nas** command is performed when the Cisco router starts up, it will not take effect until you enter a **copy running-config startup-config** command.

Configure Router to Expand Network Access Server Port Information

There are some situations when PPP or login authentication occurs on an interface different from the interface on which the call itself comes in. For example, in a V.120 ISDN call, login or PPP authentication occurs on a virtual asynchronous interface “ttt” but the call itself occurs on one of the channels of the ISDN interface.

The **radius-server attribute nas-port extended** command configures RADIUS to expand the size of the NAS-Port attribute (RADIUS IETF Attribute 5) field to 32 bits. The upper 16 bits of the NAS-Port attribute display the type and number of the controlling interface; the lower 16 bits indicate the interface undergoing authentication.

To display expanded interface information in the NAS-Port attribute field, perform the following task in global configuration mode:

Task	Command
Expand the size of the NAS-Port attribute from 16 to 32 bits to display extended interface information.	**radius-server attribute nas-port extended**

Note This command replaces the deprecated **radius-server extended-portnames** command.

On platforms with multiple interfaces (ports) per slot, the Cisco RADIUS implementation will not provide a unique NAS-Port attribute that permits distinguishing between the interfaces. For example, if a dual PRI interface is in slot 1, calls on both Serial1/0:1 and Serial1/1:1 will appear as NAS-Port = 20101.

Once again, this is because of the 16-bit field size limitation associated with RADIUS IETF NAS-port attribute. In this case, the solution is to replace the NAS-port attribute with a vendor-specific attribute (RADIUS IETF Attribute 26). Cisco's vendor-ID is 9, and the Cisco-NAS-Port attribute is subtype 2. Vendor-specific attributes (VSAs) can be turned on by entering the **radius-server vsa send** command. The port information in this attribute is provided and configured using the **aaa nas port extended** command.

To replace the NAS-Port attribute with RADIUS IETF Attribute 26 and to display extended field information, perform the following tasks in global configuration mode:

Task	Command
Enable the network access server to recognize and use vendor-specific attributes as defined by RADIUS IETF Attribute 26.	**radius-server vsa send [accounting | authentication]**
Expand the size of the VSA nas-port field from 16 to 32 bits to display extended interface information.	**aaa nas-port extended**

The standard NAS-Port attribute (RADIUS IETF Attribute 5) will continue to be sent. If you don't want this information to be sent, you can suppress it by using the **no radius-server attribute nas-port** command. When this command is configured, the standard NAS-Port attribute will no longer be sent.

For a complete list of RADIUS attributes, refer to the RADIUS attributes appendix.

Specify RADIUS Authentication

After you have identified the RADIUS server and defined the RADIUS authentication key, you need to define method lists for RADIUS authentication. Because RADIUS authentication is facilitated through AAA, you need to enter the **aaa authentication** command, specifying RADIUS as the authentication method. For more information, refer to the "Configuring Authentication" chapter in the *Security Configuration Guide*.

Specify RADIUS Authorization

AAA authorization lets you set parameters that restrict a user's network access. Authorization using RADIUS provides one method for remote access control, including one-time authorization or authorization for each service, per-user account list and profile, user group support, and support of IP, IPX, ARA, and Telnet. Because RADIUS authorization is facilitated through AAA, you need to issue the **aaa authorization** command, specifying RADIUS as the authorization method. For more information, refer to the "Configuring Authorization" chapter.

Specify RADIUS Accounting

The AAA accounting feature enables you to track the services users are accessing as well as the amount of network resources they are consuming. Because RADIUS accounting is facilitated through AAA, you need to issue the **aaa accounting** command, specifying RADIUS as the accounting method. For more information, refer to the "Configuring Accounting" chapter.

RADIUS Attributes

The network access server monitors the RADIUS authorization and accounting functions defined by RADIUS attributes in each user-profile. For a list of supported RADIUS attributes, refer to the "RADIUS Attributes" appendix.

Vendor-Proprietary RADIUS Attributes

An Internet Engineering Task Force (IETF) draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the network access server and the RADIUS server. Some vendors, nevertheless, have extended the RADIUS attribute set in a unique way. Cisco IOS software supports a subset of vendor-proprietary RADIUS attributes. For a list of supported vendor-proprietary RADIUS attributes, refer to the “RADIUS Attributes” appendix.

RADIUS Configuration Examples

RADIUS configuration examples in this section include the following:

- RADIUS Authentication and Authorization Example
- RADIUS Authentication, Authorization, and Accounting Example
- Vendor-Proprietary RADIUS Configuration Example

RADIUS Authentication and Authorization Example

The following example shows how to configure the router to authenticate and authorize using RADIUS:

```
aaa authentication login use-radius radius local
aaa authentication ppp user-radius if-needed radius
aaa authorization exec radius
aaa authorization network radius
```

The lines in this sample RADIUS authentication and authorization configuration are defined as follows:

- The **aaa authentication login use-radius radius local** command configures the router to use RADIUS for authentication at the login prompt. If RADIUS returns an error, the user is authenticated using the local database. In this example, **use-radius** is the name of the method list, which specifies RADIUS and then local authentication.
- The **aaa authentication ppp user-radius if-needed radius** command configures the Cisco IOS software to use RADIUS authentication for lines using Point-to-Point Protocol (PPP) with CHAP or PAP if the user has not already been authorized. If the EXEC facility has authenticated the user, RADIUS authentication is not performed. In this example, **user-radius** is the name of the method list defining RADIUS as the if-needed authentication method.
- The **aaa authorization exec radius** command sets the RADIUS information that is used for EXEC authorization, autocommands, and access lists.
- The **aaa authorization network radius** command sets RADIUS for network authorization, address assignment, and access lists.

RADIUS Authentication, Authorization, and Accounting Example

The following sample is a general configuration using RADIUS with the AAA command set:

```
radius-server host 123.45.1.2
radius-server key myRaDiUSpassWoRd
username root password ALongPassword
aaa authentication ppp dialins radius local
aaa authorization network radius local
aaa accounting network start-stop radius
aaa authentication login admins local
aaa authorization exec local
line 1 16
 autoselect ppp
 autoselect during-login
 login authentication admins
 modem ri-is-cd
interface group-async 1
 encaps ppp
 ppp authentication pap dialins
```

The lines in this sample RADIUS authentication, authorization, and accounting configuration are defined as follows:

- The **radius-server host** command defines the IP address of the RADIUS server host.
- The **radius-server key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **aaa authentication ppp dialins radius local** command defines the authentication method list "dialins," which specifies that RADIUS authentication, then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP.
- The **ppp authentication pap dialins** command applies the "dialins" method list to the lines specified.
- The **aaa authorization network radius local** command is used to assign an address and other network parameters to the RADIUS user.
- The **aaa accounting network start-stop radius** command tracks PPP usage.
- The **aaa authentication login admins local** command defines another method list, "admins," for login authentication.
- The **login authentication admins** command applies the "admins" method list for login authentication.

Vendor-Proprietary RADIUS Configuration Example

The following sample is a general configuration using vendor-proprietary RADIUS with the AAA command set:

```
radius-server host alcatraz non-standard
radius-server key myRaDiUSpassWoRd
radius-server configure-nas
username root password ALongPassword
aaa authentication ppp dialins radius local
aaa authorization network radius local
aaa accounting network start-stop radius
aaa authentication login admins local
aaa authorization exec local
line 1 16
autoselect ppp
autoselect during-login
login authentication admins
modem ri-is-cd
interface group-async 1
encaps ppp
ppp authentication pap dialins
```

The lines in this sample RADIUS authentication, authorization, and accounting configuration are defined as follows:

- The **radius-server host non-standard** command defines the name of the RADIUS server host and identifies that this RADIUS host uses a vendor-proprietary version of RADIUS.
- The **radius-server key** command defines the shared secret text string between the network access server and the RADIUS server host.
- The **radius-server configure-nas** command defines that the Cisco router or access server will query the RADIUS server for static routes and IP pool definitions when the device first starts up.
- The **aaa authentication ppp dialins radius local** command defines the authentication method list “dialins,” which specifies that RADIUS authentication, then (if the RADIUS server does not respond) local authentication will be used on serial lines using PPP.
- The **ppp authentication pap dialins** command applies the “dialins” method list to the lines specified.
- The **aaa authorization network radius local** command is used to assign an address and other network parameters to the RADIUS user.
- The **aaa accounting network start-stop radius** command tracks PPP usage.
- The **aaa authentication login admins local** command defines another method list, “admins,” for login authentication.
- The **login authentication admins** command applies the “admins” method list for login authentication.