



Configuring RADIUS and TACACS+ Servers

This chapter describes how to enable and configure the Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+), which provide detailed accounting information and flexible administrative control over authentication and authorization processes. RADIUS and TACACS+ are facilitated through AAA and can be enabled only through AAA commands.



Note

For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Security Command Reference for Release 12.2*.

This chapter contains these sections:

- [Configuring and Enabling RADIUS, page 11-2](#)
- [Configuring and Enabling TACACS+, page 11-16](#)

Configuring and Enabling RADIUS

This section describes how to configure and enable RADIUS. These sections describe RADIUS configuration:

- [Understanding RADIUS, page 11-2](#)
- [RADIUS Operation, page 11-3](#)
- [Configuring RADIUS, page 11-4](#)
- [Displaying the RADIUS Configuration, page 11-15](#)

Understanding RADIUS

RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on supported Cisco devices and send authentication requests to a central RADIUS server, which contains all user authentication and network service access information. The RADIUS host is normally a multiuser system running RADIUS server software from Cisco (Cisco Secure Access Control Server version 3.0), Livingston, Merit, Microsoft, or another software provider. For more information, refer to the RADIUS server documentation.

Use RADIUS in these network environments, which 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 is customized to work with the Kerberos security system.
- Turnkey network security environments in which applications support the RADIUS protocol, such as 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 to grant access to network resources.
- Networks already using RADIUS. You can add a Cisco bridge containing a RADIUS client to the network.
- Networks that require resource accounting. You can use RADIUS accounting independently of RADIUS authentication or authorization. The RADIUS accounting functions allow data to be sent at the start and end of services, showing the amount of resources (such as time, packets, bytes, and so forth) used during the session. An Internet service provider might use a freeware-based version of RADIUS access control and accounting software to meet special security and billing needs.

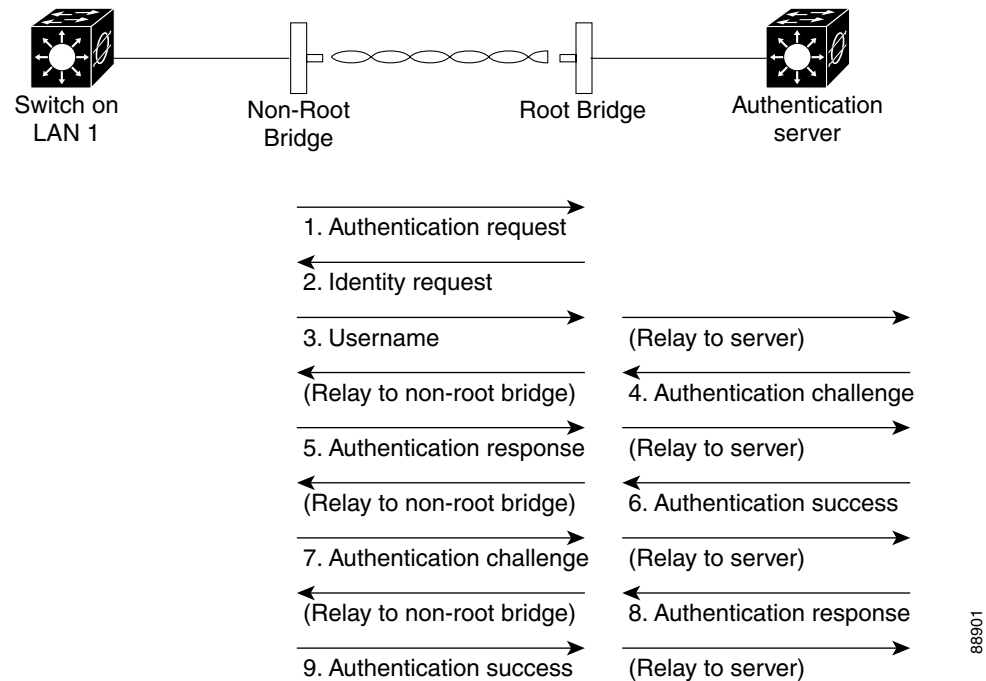
RADIUS is not suitable in these network security situations:

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

RADIUS Operation

When a non-root bridge attempts to authenticate to a bridge whose access is controlled by a RADIUS server, authentication to the network occurs in the steps shown in [Figure 11-1](#):

Figure 11-1 Sequence for EAP Authentication



In Steps 1 through 9 in [Figure 11-1](#), a non-root bridge and a RADIUS server on the wired LAN use 802.1x and EAP to perform a mutual authentication through the root bridge. The RADIUS server sends an authentication challenge to the non-root bridge. The non-root bridge uses a one-way encryption of the user-supplied password to generate a response to the challenge and sends that response to the RADIUS server. Using information from its user database, the RADIUS server creates its own response and compares that to the response from the non-root bridge. When the RADIUS server authenticates the non-root bridge, the process repeats in reverse, and the non-root bridge authenticates the RADIUS server.

When mutual authentication is complete, the RADIUS server and the non-root bridge determine a WEP key that is unique to the non-root bridge and provides the non-root bridge with the appropriate level of network access, thereby approximating the level of security in a wired switched segment to an individual desktop. The non-root bridge loads this key and prepares to use it for the logon session.

During the logon session, the RADIUS server encrypts and sends the WEP key, called a *session key*, over the wired LAN to the root bridge. The root bridge encrypts its broadcast key with the session key and sends the encrypted broadcast key to the non-root bridge, which uses the session key to decrypt it. The non-root bridge and the root bridge activate WEP and use the session and broadcast WEP keys for all communications during the remainder of the session.

There is more than one type of EAP authentication, but the root bridge behaves the same way for each type: it relays authentication messages from the non-root bridge to the RADIUS server and from the RADIUS server to the non-root bridge. See the [“Assigning Authentication Types to an SSID”](#) section on [page 10-5](#) for instructions on setting up authentication using a RADIUS server.

Configuring RADIUS

This section describes how to configure your bridge to support RADIUS. At a minimum, you must identify the host or hosts that run the RADIUS server software and define the method lists for RADIUS authentication. You can optionally define method lists for RADIUS authorization and accounting.

A method list defines the sequence and methods to be used to authenticate, to authorize, or to keep accounts on a non-root bridge. You can use method lists to designate one or more security protocols to be used, thus ensuring a backup system if the initial method fails. The software uses the first method listed to authenticate, to authorize, or to keep accounts on non-root bridges; if that method does not respond, the software selects the next method in the list. This process continues until there is successful communication with a listed method or the method list is exhausted.

You should have access to and should configure a RADIUS server before configuring RADIUS features on your bridge.

This section contains this configuration information:

- [Default RADIUS Configuration, page 11-4](#)
- [Identifying the RADIUS Server Host, page 11-4](#) (required)
- [Configuring RADIUS Login Authentication, page 11-7](#) (required)
- [Defining AAA Server Groups, page 11-9](#) (optional)
- [Configuring RADIUS Authorization for User Privileged Access and Network Services, page 11-11](#) (optional)
- [Starting RADIUS Accounting, page 11-12](#) (optional)
- [Configuring Settings for All RADIUS Servers, page 11-13](#) (optional)
- [Configuring the Bridge to Use Vendor-Specific RADIUS Attributes, page 11-13](#) (optional)
- [Configuring the Bridge for Vendor-Proprietary RADIUS Server Communication, page 11-14](#) (optional)

**Note**

The RADIUS server CLI commands are disabled until you enter the **aaa new-model** command.

Default RADIUS Configuration

RADIUS and AAA are disabled by default.

To prevent a lapse in security, you cannot configure RADIUS through a network management application. When enabled, RADIUS can authenticate users accessing the bridge through the CLI.

Identifying the RADIUS Server Host

Access point-to-RADIUS-server communication involves several components:

- Host name or IP address
- Authentication destination port
- Accounting destination port
- Key string
- Timeout period

- Retransmission value

You identify RADIUS security servers by their host name or IP address, host name and specific UDP port numbers, or their IP address and specific UDP port numbers. The combination of the IP address and the UDP port number creates a unique identifier allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. This unique identifier enables RADIUS requests to be sent to multiple UDP ports on a server at the same IP address.

If two different host entries on the same RADIUS server are configured for the same service—such as accounting—the second host entry configured acts as a fail-over backup to the first one. Using this example, if the first host entry fails to provide accounting services, the bridge tries the second host entry configured on the same device for accounting services. (The RADIUS host entries are tried in the order that they are configured.)

A RADIUS server and the bridge 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 (key) string that it shares with the bridge.

The timeout, retransmission, and encryption key values can be configured globally per server for all RADIUS servers or in some combination of global and per-server settings. To apply these settings globally to all RADIUS servers communicating with the bridge, use the three unique global configuration commands: **radius-server timeout**, **radius-server retransmit**, and **radius-server key**. To apply these values on a specific RADIUS server, use the **radius-server host** global configuration command.


Note

If you configure both global and per-server functions (timeout, retransmission, and key commands) on the bridge, the per-server timer, retransmission, and key value commands override global timer, retransmission, and key value commands. For information on configuring these setting on all RADIUS servers, see the [“Configuring Settings for All RADIUS Servers” section on page 11-13](#).

You can configure the bridge to use AAA server groups to group existing server hosts for authentication. For more information, see the [“Defining AAA Server Groups” section on page 11-9](#).

Beginning in privileged EXEC mode, follow these steps to configure per-server RADIUS server communication. This procedure is required.

| | Command | Purpose |
|--------|---------------------------|----------------------------------|
| Step 1 | configure terminal | Enter global configuration mode. |
| Step 2 | aaa new-model | Enable AAA. |

| Command | Purpose |
|--|---|
| Step 3 radius-server host { <i>hostname</i> <i>ip-address</i> } [auth-port <i>port-number</i>] [acct-port <i>port-number</i>] [timeout <i>seconds</i>] [retransmit <i>retries</i>] [key <i>string</i>] | <p>Specify the IP address or host name of the remote RADIUS server host.</p> <ul style="list-style-type: none"> (Optional) For auth-port <i>port-number</i>, specify the UDP destination port for authentication requests. (Optional) For acct-port <i>port-number</i>, specify the UDP destination port for accounting requests. (Optional) For timeout <i>seconds</i>, specify the time interval that the bridge waits for the RADIUS server to reply before retransmitting. The range is 1 to 1000. This setting overrides the radius-server timeout global configuration command setting. If no timeout is set with the radius-server host command, the setting of the radius-server timeout command is used. (Optional) For retransmit <i>retries</i>, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the radius-server host command, the setting of the radius-server retransmit global configuration command is used. (Optional) For key <i>string</i>, specify the authentication and encryption key used between the bridge and the RADIUS daemon running on the RADIUS server. <p>Note The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the radius-server host command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.</p> <p>To configure the bridge to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The bridge software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.</p> |
| Step 4 end | Return to privileged EXEC mode. |
| Step 5 show running-config | Verify your entries. |
| Step 6 copy running-config startup-config | (Optional) Save your entries in the configuration file. |

To remove the specified RADIUS server, use the **no radius-server host** *hostname* | *ip-address* global configuration command.

This example shows how to configure one RADIUS server to be used for authentication and another to be used for accounting:

```
BR(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
BR(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```

This example shows how to configure *host1* as the RADIUS server and to use the default ports for both authentication and accounting:

```
BR(config)# radius-server host host1
```



Note

You also need to configure some settings on the RADIUS server. These settings include the IP address of the bridge and the key string to be shared by both the server and the bridge. For more information, refer to the RADIUS server documentation.

Configuring RADIUS Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific interface before any of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named *default*). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined.

A method list describes the sequence and authentication methods to be queried to authenticate a user (in this case, a non-root bridge). You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the user access—the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure login authentication. This procedure is required.

| | Command | Purpose |
|--------|---------------------------------|----------------------------------|
| Step 1 | <code>configure terminal</code> | Enter global configuration mode. |
| Step 2 | <code>aaa new-model</code> | Enable AAA. |

| | Command | Purpose |
|--------|--|--|
| Step 3 | aaa authentication login { default <i>list-name</i> } <i>method1</i> [<i>method2...</i>] | <p>Create a login authentication method list.</p> <ul style="list-style-type: none"> To create a default list that is used when a named list is <i>not</i> specified in the login authentication command, use the default keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. For more information on list names, click this link: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgr/fsecur_c/fsaaa/scfathen.htm#xtocid2 For <i>method1...</i>, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. <p>Select one of these methods:</p> <ul style="list-style-type: none"> line—Use the line password for authentication. You must define a line password before you can use this authentication method. Use the password <i>password</i> line configuration command. local—Use the local username database for authentication. You must enter username information in the database. Use the username <i>password</i> global configuration command. radius—Use RADIUS authentication. You must configure the RADIUS server before you can use this authentication method. For more information, see the “Identifying the RADIUS Server Host” section on page 11-4. |
| Step 4 | line [console tty vty] <i>line-number</i> [<i>ending-line-number</i>] | Enter line configuration mode, and configure the lines to which you want to apply the authentication list. |
| Step 5 | login authentication { default <i>list-name</i> } | <p>Apply the authentication list to a line or set of lines.</p> <ul style="list-style-type: none"> If you specify default, use the default list created with the aaa authentication login command. For <i>list-name</i>, specify the list created with the aaa authentication login command. |
| Step 6 | radius-server attribute 32 include-in-access-req format %h | Configure the bridge to send its system name in the NAS_ID attribute for authentication. |
| Step 7 | end | Return to privileged EXEC mode. |
| Step 8 | show running-config | Verify your entries. |
| Step 9 | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

To disable AAA, use the **no aaa new-model** global configuration command. To disable AAA authentication, use the **no aaa authentication login** { **default** | *list-name* } *method1* [*method2...*] global configuration command. To either disable RADIUS authentication for logins or to return to the default value, use the **no login authentication** { **default** | *list-name* } line configuration command.

Defining AAA Server Groups

You can configure the bridge to use AAA server groups to group existing server hosts for authentication. You select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list, which lists the IP addresses of the selected server hosts.

Server groups also can include multiple host entries for the same server if each entry has a unique identifier (the combination of the IP address and UDP port number), allowing different ports to be individually defined as RADIUS hosts providing a specific AAA service. If you configure two different host entries on the same RADIUS server for the same service (such as accounting), the second configured host entry acts as a fail-over backup to the first one.

You use the **server** group server configuration command to associate a particular server with a defined group server. You can either identify the server by its IP address or identify multiple host instances or entries by using the optional **auth-port** and **acct-port** keywords.

Beginning in privileged EXEC mode, follow these steps to define the AAA server group and associate a particular RADIUS server with it:

| | Command | Purpose |
|--------|---------------------------|----------------------------------|
| Step 1 | configure terminal | Enter global configuration mode. |
| Step 2 | aaa new-model | Enable AAA. |

| Command | Purpose |
|--|---|
| Step 3 radius-server host { <i>hostname</i> <i>ip-address</i> } [auth-port <i>port-number</i>] [acct-port <i>port-number</i>] [timeout <i>seconds</i>] [retransmit <i>retries</i>] [key <i>string</i>] | <p>Specify the IP address or host name of the remote RADIUS server host.</p> <ul style="list-style-type: none"> (Optional) For auth-port <i>port-number</i>, specify the UDP destination port for authentication requests. (Optional) For acct-port <i>port-number</i>, specify the UDP destination port for accounting requests. (Optional) For timeout <i>seconds</i>, specify the time interval that the bridge waits for the RADIUS server to reply before retransmitting. The range is 1 to 1000. This setting overrides the radius-server timeout global configuration command setting. If no timeout is set with the radius-server host command, the setting of the radius-server timeout command is used. (Optional) For retransmit <i>retries</i>, specify the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly. The range is 1 to 1000. If no retransmit value is set with the radius-server host command, the setting of the radius-server retransmit global configuration command is used. (Optional) For key <i>string</i>, specify the authentication and encryption key used between the bridge and the RADIUS daemon running on the RADIUS server. <p>Note The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the radius-server host command. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key.</p> <p>To configure the bridge to recognize more than one host entry associated with a single IP address, enter this command as many times as necessary, making sure that each UDP port number is different. The bridge software searches for hosts in the order in which you specify them. Set the timeout, retransmit, and encryption key values to use with the specific RADIUS host.</p> |
| Step 4 aaa group server radius <i>group-name</i> | <p>Define the AAA server-group with a group name.</p> <p>This command puts the bridge in a server group configuration mode.</p> |
| Step 5 server <i>ip-address</i> | <p>Associate a particular RADIUS server with the defined server group. Repeat this step for each RADIUS server in the AAA server group.</p> <p>Each server in the group must be previously defined in Step 2.</p> |
| Step 6 end | <p>Return to privileged EXEC mode.</p> |
| Step 7 show running-config | <p>Verify your entries.</p> |
| Step 8 copy running-config startup-config | <p>(Optional) Save your entries in the configuration file.</p> |
| Step 9 | <p>Enable RADIUS login authentication. See the “Configuring RADIUS Login Authentication” section on page 11-7.</p> |

To remove the specified RADIUS server, use the **no radius-server host** *hostname | ip-address* global configuration command. To remove a server group from the configuration list, use the **no aaa group server radius** *group-name* global configuration command. To remove the IP address of a RADIUS server, use the **no server ip-address** server group configuration command.

In this example, the bridge is configured to recognize two different RADIUS group servers (*group1* and *group2*). Group1 has two different host entries on the same RADIUS server configured for the same services. The second host entry acts as a fail-over backup to the first entry.

```
BR(config)# aaa new-model
BR(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
BR(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
BR(config)# aaa group server radius group1
BR(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
BR(config-sg-radius)# exit
BR(config)# aaa group server radius group2
BR(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
BR(config-sg-radius)# exit
```

Configuring RADIUS Authorization for User Privileged Access and Network Services

AAA authorization limits the services available to a user. When AAA authorization is enabled, the bridge uses information retrieved from the user's profile, which is in the local user database or on the security server, to configure the user's session. The user is granted access to a requested service only if the information in the user profile allows it.



Note

This section describes setting up authorization for bridge administrators.

You can use the **aaa authorization** global configuration command with the **radius** keyword to set parameters that restrict a user's network access to privileged EXEC mode.

The **aaa authorization exec radius local** command sets these authorization parameters:

- Use RADIUS for privileged EXEC access authorization if authentication was performed by using RADIUS.
- Use the local database if authentication was not performed by using RADIUS.



Note

Authorization is bypassed for authenticated users who log in through the CLI even if authorization has been configured.

Beginning in privileged EXEC mode, follow these steps to specify RADIUS authorization for privileged EXEC access and network services:

| | Command | Purpose |
|--------|---|--|
| Step 1 | configure terminal | Enter global configuration mode. |
| Step 2 | aaa authorization network radius | Configure the bridge for user RADIUS authorization for all network-related service requests. |
| Step 3 | aaa authorization exec radius | Configure the bridge for user RADIUS authorization to determine if the user has privileged EXEC access. The exec keyword might return user profile information (such as autocommand information). |
| Step 4 | end | Return to privileged EXEC mode. |
| Step 5 | show running-config | Verify your entries. |
| Step 6 | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

To disable authorization, use the **no aaa authorization {network | exec} method1** global configuration command.

Starting RADIUS Accounting

The AAA accounting feature tracks the services that users are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the bridge reports user activity to the RADIUS security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, or auditing.

Beginning in privileged EXEC mode, follow these steps to enable RADIUS accounting for each Cisco IOS privilege level and for network services:

| | Command | Purpose |
|--------|--|---|
| Step 1 | configure terminal | Enter global configuration mode. |
| Step 2 | aaa accounting network start-stop radius | Enable RADIUS accounting for all network-related service requests. |
| Step 3 | ip radius source-interface bvi1 | Configure the bridge to send its BVI IP address in the NAS_IP_ADDRESS attribute for accounting records. |
| Step 4 | aaa accounting update periodic <i>minutes</i> | Enter an accounting update interval in minutes. |
| Step 5 | end | Return to privileged EXEC mode. |
| Step 6 | show running-config | Verify your entries. |
| Step 7 | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

To disable accounting, use the **no aaa accounting {network | exec} {start-stop} method1...** global configuration command.

Configuring Settings for All RADIUS Servers

Beginning in privileged EXEC mode, follow these steps to configure global communication settings between the bridge and all RADIUS servers:

| | Command | Purpose |
|--------|---|---|
| Step 1 | configure terminal | Enter global configuration mode. |
| Step 2 | radius-server key <i>string</i> | Specify the shared secret text string used between the bridge and all RADIUS servers. Note The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. |
| Step 3 | radius-server retransmit <i>retries</i> | Specify the number of times the bridge sends each RADIUS request to the server before giving up. The default is 3; the range 1 to 1000. |
| Step 4 | radius-server timeout <i>seconds</i> | Specify the number of seconds an bridge waits for a reply to a RADIUS request before resending the request. The default is 5 seconds; the range is 1 to 1000. |
| Step 5 | radius-server deadtime <i>minutes</i> | Use this command to cause the Cisco IOS software to mark as “dead” any RADIUS servers that fail to respond to authentication requests, thus avoiding the wait for the request to time out before trying the next configured server. A RADIUS server marked as dead is skipped by additional requests for the duration of minutes that you specify, or unless there are no servers not marked dead. Note If you set up more than one RADIUS server, you must configure the RADIUS server deadtime for optimal performance. |
| Step 6 | radius-server attribute 32 include-in-access-req format %h | Configure the bridge to send its system name in the NAS_ID attribute for authentication. |
| Step 7 | end | Return to privileged EXEC mode. |
| Step 8 | show running-config | Verify your settings. |
| Step 9 | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

To return to the default setting for the retransmit, timeout, and deadtime, use the **no** forms of these commands.

Configuring the Bridge to Use Vendor-Specific RADIUS Attributes

The Internet Engineering Task Force (IETF) draft standard specifies a method for communicating vendor-specific information between the bridge 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 by 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 with this 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 AV pair defined in the Cisco TACACS+ specification, and *sep* is = for mandatory attributes and the asterisk (*) 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 activates Cisco's *multiple named ip address pools* feature during IP authorization (during PPP's IPCP address assignment):

```
cisco-avpair= "ip:addr-pool=first"
```

The following example shows how to provide a user logging in from an bridge with immediate access to privileged 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)."

Beginning in privileged EXEC mode, follow these steps to configure the bridge to recognize and use VSAs:

| | Command | Purpose |
|--------|---|--|
| Step 1 | configure terminal | Enter global configuration mode. |
| Step 2 | radius-server vsa send [accounting authentication] | Enable the bridge to recognize and use VSAs as defined by RADIUS IETF attribute 26. <ul style="list-style-type: none"> (Optional) Use the accounting keyword to limit the set of recognized vendor-specific attributes to only accounting attributes. (Optional) Use the authentication keyword to limit the set of recognized vendor-specific attributes to only authentication attributes. If you enter this command without keywords, both accounting and authentication vendor-specific attributes are used. |
| Step 3 | end | Return to privileged EXEC mode. |
| Step 4 | show running-config | Verify your settings. |
| Step 5 | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

For a complete list of RADIUS attributes or more information about VSA 26, refer to the "RADIUS Attributes" appendix in the *Cisco IOS Security Configuration Guide for Release 12.2*.

Configuring the Bridge for Vendor-Proprietary RADIUS Server Communication

Although an IETF draft standard for RADIUS specifies a method for communicating vendor-proprietary information between the bridge 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 bridge. You specify the RADIUS host and secret text string by using the **radius-server** global configuration commands.

Beginning in privileged EXEC mode, follow these steps to specify a vendor-proprietary RADIUS server host and a shared secret text string:

| | Command | Purpose |
|--------|---|---|
| Step 1 | configure terminal | Enter global configuration mode. |
| Step 2 | radius-server host { <i>hostname</i> <i>ip-address</i> } non-standard | 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. |
| Step 3 | radius-server key <i>string</i> | Specify the shared secret text string used between the bridge and the vendor-proprietary RADIUS server. The bridge and the RADIUS server use this text string to encrypt passwords and exchange responses. Note The key is a text string that must match the encryption key used on the RADIUS server. Leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks are part of the key. |
| Step 4 | end | Return to privileged EXEC mode. |
| Step 5 | show running-config | Verify your settings. |
| Step 6 | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

To delete the vendor-proprietary RADIUS host, use the **no radius-server host** {*hostname* | *ip-address*} **non-standard** global configuration command. To disable the key, use the **no radius-server key** global configuration command.

This example shows how to specify a vendor-proprietary RADIUS host and to use a secret key of *rad124* between the bridge and the server:

```
BR(config)# radius-server host 172.20.30.15 nonstandard
BR(config)# radius-server key rad124
```

Displaying the RADIUS Configuration

To display the RADIUS configuration, use the **show running-config** privileged EXEC command.

Configuring and Enabling TACACS+

This section contains this configuration information:

- [Understanding TACACS+, page 11-16](#)
- [TACACS+ Operation, page 11-17](#)
- [Configuring TACACS+, page 11-17](#)
- [Displaying the TACACS+ Configuration, page 11-22](#)

Understanding TACACS+

TACACS+ is a security application that provides centralized validation of users attempting to gain access to your bridge. Unlike RADIUS, TACACS+ does not authenticate non-root bridges associated to the root bridge.

TACACS+ services are maintained in a database on a TACACS+ daemon typically running on a UNIX or Windows NT workstation. You should have access to and should configure a TACACS+ server before configuring TACACS+ features on your bridge.

TACACS+ provides for separate and modular authentication, authorization, and accounting facilities. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide each service—authentication, authorization, and accounting—independently. Each service can be tied into its own database to take advantage of other services available on that server or on the network, depending on the capabilities of the daemon.

TACACS+, administered through the AAA security services, can provide these services:

- **Authentication**—Provides complete control of authentication of administrators through login and password dialog, challenge and response, and messaging support.
The authentication facility can conduct a dialog with the administrator (for example, after a username and password are provided, to challenge a user with several questions, such as home address, mother's maiden name, service type, and social security number). The TACACS+ authentication service can also send messages to administrator screens. For example, a message could notify administrators that their passwords must be changed because of the company's password aging policy.
- **Authorization**—Provides fine-grained control over administrator capabilities for the duration of the administrator's session, including but not limited to setting autocommands, access control, session duration, or protocol support. You can also enforce restrictions on the commands that an administrator can execute with the TACACS+ authorization feature.
- **Accounting**—Collects and sends information used for billing, auditing, and reporting to the TACACS+ daemon. Network managers can use the accounting facility to track administrator activity for a security audit or to provide information for user billing. Accounting records include administrator identities, start and stop times, executed commands (such as PPP), number of packets, and number of bytes.

The TACACS+ protocol provides authentication between the bridge and the TACACS+ daemon, and it ensures confidentiality because all protocol exchanges between the bridge and the TACACS+ daemon are encrypted.

You need a system running the TACACS+ daemon software to use TACACS+ on your bridge.

TACACS+ Operation

When an administrator attempts a simple ASCII login by authenticating to a bridge using TACACS+, this process occurs:

1. When the connection is established, the bridge contacts the TACACS+ daemon to obtain a username prompt, which is then displayed to the administrator. The administrator enters a username, and the bridge then contacts the TACACS+ daemon to obtain a password prompt. The bridge displays the password prompt to the administrator, the administrator enters a password, and the password is then sent to the TACACS+ daemon.

TACACS+ allows a conversation to be held between the daemon and the administrator until the daemon receives enough information to authenticate the administrator. The daemon prompts for a username and password combination, but can include other items, such as the user's mother's maiden name.

2. The bridge eventually receives one of these responses from the TACACS+ daemon:
 - ACCEPT—The administrator is authenticated and service can begin. If the bridge is configured to require authorization, authorization begins at this time.
 - REJECT—The administrator is not authenticated. The administrator can be denied access or is prompted to retry the login sequence, depending on the TACACS+ daemon.
 - ERROR—An error occurred at some time during authentication with the daemon or in the network connection between the daemon and the bridge. If an ERROR response is received, the bridge typically tries to use an alternative method for authenticating the administrator.
 - CONTINUE—The administrator is prompted for additional authentication information.

After authentication, the administrator undergoes an additional authorization phase if authorization has been enabled on the bridge. Administrators must first successfully complete TACACS+ authentication before proceeding to TACACS+ authorization.

3. If TACACS+ authorization is required, the TACACS+ daemon is again contacted, and it returns an ACCEPT or REJECT authorization response. If an ACCEPT response is returned, the response contains data in the form of attributes that direct the EXEC or NETWORK session for that administrator, determining the services that the administrator can access:
 - Telnet, rlogin, or privileged EXEC services
 - Connection parameters, including the host or client IP address, access list, and administrator timeouts

Configuring TACACS+

This section describes how to configure your bridge to support TACACS+. At a minimum, you must identify the host or hosts maintaining the TACACS+ daemon and define the method lists for TACACS+ authentication. You can optionally define method lists for TACACS+ authorization and accounting. A method list defines the sequence and methods to be used to authenticate, to authorize, or to keep accounts on an administrator. You can use method lists to designate one or more security protocols to be used, thus ensuring a backup system if the initial method fails. The software uses the first method listed to authenticate, to authorize, or to keep accounts on administrators; if that method does not respond, the software selects the next method in the list. This process continues until there is successful communication with a listed method or the method list is exhausted.

This section contains this configuration information:

- [Default TACACS+ Configuration, page 11-18](#)
- [Identifying the TACACS+ Server Host and Setting the Authentication Key, page 11-18](#)
- [Configuring TACACS+ Login Authentication, page 11-19](#)
- [Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services, page 11-20](#)
- [Starting TACACS+ Accounting, page 11-21](#)

Default TACACS+ Configuration

TACACS+ and AAA are disabled by default.

To prevent a lapse in security, you cannot configure TACACS+ through a network management application. When enabled, TACACS+ can authenticate administrators accessing the bridge through the CLI.

Identifying the TACACS+ Server Host and Setting the Authentication Key

You can configure the bridge to use a single server or AAA server groups to group existing server hosts for authentication. You can group servers to select a subset of the configured server hosts and use them for a particular service. The server group is used with a global server-host list and contains the list of IP addresses of the selected server hosts.

Beginning in privileged EXEC mode, follow these steps to identify the IP host or host maintaining TACACS+ server and optionally set the encryption key:

| | Command | Purpose |
|--------|---|---|
| Step 1 | configure terminal | Enter global configuration mode. |
| Step 2 | tacacs-server host <i>hostname</i> [port <i>integer</i>] [timeout <i>integer</i>] [key <i>string</i>] | Identify the IP host or hosts maintaining a TACACS+ server. Enter this command multiple times to create a list of preferred hosts. The software searches for hosts in the order in which you specify them. <ul style="list-style-type: none"> • For <i>hostname</i>, specify the name or IP address of the host. • (Optional) For port <i>integer</i>, specify a server port number. The default is port 49. The range is 1 to 65535. • (Optional) For timeout <i>integer</i>, specify a time in seconds the bridge waits for a response from the daemon before it times out and declares an error. The default is 5 seconds. The range is 1 to 1000 seconds. • (Optional) For key <i>string</i>, specify the encryption key for encrypting and decrypting all traffic between the bridge and the TACACS+ daemon. You must configure the same key on the TACACS+ daemon for encryption to be successful. |
| Step 3 | aaa new-model | Enable AAA. |
| Step 4 | aaa group server tacacs+ <i>group-name</i> | (Optional) Define the AAA server-group with a group name. This command puts the bridge in a server group subconfiguration mode. |

| | Command | Purpose |
|--------|---|---|
| Step 5 | <code>server ip-address</code> | (Optional) Associate a particular TACACS+ server with the defined server group. Repeat this step for each TACACS+ server in the AAA server group. Each server in the group must be previously defined in Step 2. |
| Step 6 | <code>end</code> | Return to privileged EXEC mode. |
| Step 7 | <code>show tacacs</code> | Verify your entries. |
| Step 8 | <code>copy running-config startup-config</code> | (Optional) Save your entries in the configuration file. |

To remove the specified TACACS+ server name or address, use the **no tacacs-server host hostname** global configuration command. To remove a server group from the configuration list, use the **no aaa group server tacacs+ group-name** global configuration command. To remove the IP address of a TACACS+ server, use the **no server ip-address** server group subconfiguration command.

Configuring TACACS+ Login Authentication

To configure AAA authentication, you define a named list of authentication methods and then apply that list to various interfaces. The method list defines the types of authentication to be performed and the sequence in which they are performed; it must be applied to a specific interface before any of the defined authentication methods are performed. The only exception is the default method list (which, by coincidence, is named *default*). The default method list is automatically applied to all interfaces except those that have a named method list explicitly defined. A defined method list overrides the default method list.

A method list describes the sequence and authentication methods to be queried to authenticate an administrator. You can designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The software uses the first method listed to authenticate users; if that method fails to respond, the software selects the next authentication method in the method list. This process continues until there is successful communication with a listed authentication method or until all defined methods are exhausted. If authentication fails at any point in this cycle—meaning that the security server or local username database responds by denying the administrator access—the authentication process stops, and no other authentication methods are attempted.

Beginning in privileged EXEC mode, follow these steps to configure login authentication:

| | Command | Purpose |
|--------|---------------------------------|----------------------------------|
| Step 1 | <code>configure terminal</code> | Enter global configuration mode. |
| Step 2 | <code>aaa new-model</code> | Enable AAA. |

| | Command | Purpose |
|--------|--|---|
| Step 3 | aaa authentication login { default <i>list-name</i> } <i>method1</i> [<i>method2...</i>] | <p>Create a login authentication method list.</p> <ul style="list-style-type: none"> To create a default list that is used when a named list is <i>not</i> specified in the login authentication command, use the default keyword followed by the methods that are to be used in default situations. The default method list is automatically applied to all interfaces. For <i>list-name</i>, specify a character string to name the list you are creating. For <i>method1...</i>, specify the actual method the authentication algorithm tries. The additional methods of authentication are used only if the previous method returns an error, not if it fails. <p>Select one of these methods:</p> <ul style="list-style-type: none"> line—Use the line password for authentication. You must define a line password before you can use this authentication method. Use the password <i>password</i> line configuration command. local—Use the local username database for authentication. You must enter username information into the database. Use the username <i>password</i> global configuration command. tacacs+—Uses TACACS+ authentication. You must configure the TACACS+ server before you can use this authentication method. |
| Step 4 | line [console tty vty] <i>line-number</i> [<i>ending-line-number</i>] | Enter line configuration mode, and configure the lines to which you want to apply the authentication list. |
| Step 5 | login authentication { default <i>list-name</i> } | <p>Apply the authentication list to a line or set of lines.</p> <ul style="list-style-type: none"> If you specify default, use the default list created with the aaa authentication login command. For <i>list-name</i>, specify the list created with the aaa authentication login command. |
| Step 6 | end | Return to privileged EXEC mode. |
| Step 7 | show running-config | Verify your entries. |
| Step 8 | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

To disable AAA, use the **no aaa new-model** global configuration command. To disable AAA authentication, use the **no aaa authentication login** { **default** | *list-name* } *method1* [*method2...*] global configuration command. To either disable TACACS+ authentication for logins or to return to the default value, use the **no login authentication** { **default** | *list-name* } line configuration command.

Configuring TACACS+ Authorization for Privileged EXEC Access and Network Services

AAA authorization limits the services available to an administrator. When AAA authorization is enabled, the bridge uses information retrieved from the administrator's profile, which is located either in the local user database or on the security server, to configure the administrator's session. The administrator is granted access to a requested service only if the information in the administrator profile allows it.

You can use the **aaa authorization** global configuration command with the **tacacs+** keyword to set parameters that restrict an administrator's network access to privileged EXEC mode.

The **aaa authorization exec tacacs+ local** command sets these authorization parameters:

- Use TACACS+ for privileged EXEC access authorization if authentication was performed by using TACACS+.
- Use the local database if authentication was not performed by using TACACS+.

**Note**

Authorization is bypassed for authenticated administrators who log in through the CLI even if authorization has been configured.

Beginning in privileged EXEC mode, follow these steps to specify TACACS+ authorization for privileged EXEC access and network services:

| | Command | Purpose |
|--------|---|---|
| Step 1 | configure terminal | Enter global configuration mode. |
| Step 2 | aaa authorization network tacacs+ | Configure the bridge for administrator TACACS+ authorization for all network-related service requests. |
| Step 3 | aaa authorization exec tacacs+ | Configure the bridge for administrator TACACS+ authorization to determine if the administrator has privileged EXEC access. The exec keyword might return user profile information (such as autocommand information). |
| Step 4 | end | Return to privileged EXEC mode. |
| Step 5 | show running-config | Verify your entries. |
| Step 6 | copy running-config startup-config | (Optional) Save your entries in the configuration file. |

To disable authorization, use the **no aaa authorization {network | exec} method1** global configuration command.

Starting TACACS+ Accounting

The AAA accounting feature tracks the services that administrators are accessing and the amount of network resources that they are consuming. When AAA accounting is enabled, the bridge reports administrator activity to the TACACS+ security server in the form of accounting records. Each accounting record contains accounting attribute-value (AV) pairs and is stored on the security server. This data can then be analyzed for network management, client billing, or auditing.

Beginning in privileged EXEC mode, follow these steps to enable TACACS+ accounting for each Cisco IOS privilege level and for network services:

| | Command | Purpose |
|--------|--|--|
| Step 1 | configure terminal | Enter global configuration mode. |
| Step 2 | aaa accounting network start-stop tacacs+ | Enable TACACS+ accounting for all network-related service requests. |
| Step 3 | aaa accounting exec start-stop tacacs+ | Enable TACACS+ accounting to send a start-record accounting notice at the beginning of a privileged EXEC process and a stop-record at the end. |
| Step 4 | end | Return to privileged EXEC mode. |

| | Command | Purpose |
|--------|---|---|
| Step 5 | <code>show running-config</code> | Verify your entries. |
| Step 6 | <code>copy running-config startup-config</code> | (Optional) Save your entries in the configuration file. |

To disable accounting, use the `no aaa accounting {network | exec} {start-stop} method1...` global configuration command.

Displaying the TACACS+ Configuration

To display TACACS+ server statistics, use the `show tacacs` privileged EXEC command.