



RADIUS Commands

This chapter describes the commands used to configure RADIUS.

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. Cisco supports RADIUS under its Authentication, Authorization, and Accounting (AAA) security paradigm.

For information on how to configure RADIUS, refer to the “Configuring RADIUS” chapter in the *Security Configuration Guide*. For configuration examples using the commands in this chapter, refer to the “RADIUS Configuration Examples” section located at the end of the “Configuring RADIUS” chapter in the *Security Configuration Guide*.

aaa nas-port extended

To replace the NAS-Port attribute with RADIUS IETF Attribute 26 and to display extended field information, use the **aaa nas-port extended** global configuration command. Use the **no** form of this command to not display extended field information.

aaa nas-port extended

no aaa nas-port extended

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

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.

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

Examples

The following example specifies that RADIUS will display extended interface information:

```
radius-server vsa send
aaa nas-port extended
```

Related Commands

Command	Description
radius-server extended-portnames	Displays expanded interface information in the NAS-Port attribute.
radius-server vsa send	Configures the network access server to recognize and use vendor-specific attributes.

ip radius source-interface

To force RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets, use the **ip radius source-interface** global configuration command.

ip radius source-interface *subinterface-name*

no ip radius source-interface

Syntax Description	<i>subinterface-name</i> Name of the interface that RADIUS uses for all of its outgoing packets.
---------------------------	--

Defaults	This command has no factory-assigned default.
-----------------	---

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	11.3	This command was introduced.

Usage Guidelines	Use this command to set a subinterface's IP address to be used as the source address for all outgoing RADIUS packets. This address is used as long as the interface is in the <i>up</i> state. In this way, the RADIUS server can use one IP address entry for every network access client instead of maintaining a list of IP addresses.
-------------------------	---

This command is especially useful in cases where the router has many interfaces and you want to ensure that all RADIUS packets from a particular router have the same IP address.

The specified interface must have an IP address associated with it. If the specified subinterface does not have a IP address or is in the *down* state, then RADIUS reverts to the default. To avoid this, add an IP address to the subinterface or bring the interface to the *up* state.

Examples	The following example makes RADIUS use the IP address of subinterface s2 for all outgoing RADIUS packets:
-----------------	---

```
ip radius source-interface s2
```

Related Commands	Command	Description
	ip tacacs source-interface	Uses the IP address of a specified interface for all outgoing TACACS packets.
	ip telnet source-interface	Allows a user to select an address of an interface as the source address for Telnet connections.
	ip tftp source-interface	Allows a user to select the interface whose address will be used as the source address for TFTP connections.

radius-server attribute nas-port extended

The **radius-server attribute nas-port extended** command is replaced by the **radius-server attribute nas-port format** command. See the description of the **radius-server attribute nas-port format** command in this chapter for more information.

radius-server attribute nas-port format

To select the NAS-Port format used for RADIUS accounting features, and to restore the default NAS-Port format, use the **radius-server attribute nas-port format** global configuration command. If the **no** form of this command is used, attribute 5 (NAS-Port) will no longer be sent to the RADIUS server.

radius-server attribute nas-port format *format*

no radius-server attribute nas-port format *format*

Syntax Description	<i>format</i>	NAS-Port format. Possible values for the format argument are as follows: a —Standard NAS-Port format b —Extended NAS-Port format c —Shelf-slot NAS-Port format d —PPP extended NAS-Port format
---------------------------	---------------	--

Defaults	Standard NAS-Port format
-----------------	--------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	11.3(7)T	This command was introduced.
	11.3(9)DB	The PPP extended NAS-Port format was added.

Usage Guidelines	The radius-server attribute nas-port format command configures RADIUS to change the size and format of the NAS-Port attribute field (RADIUS IETF attribute 5).
-------------------------	---

The following NAS-Port formats are supported:

- Standard NAS-Port format—This 16-bit NAS-Port format indicates the type, port, and channel of the controlling interface. This is the default format used by Cisco IOS software.
- Extended NAS-Port format—The standard NAS-Port attribute field is expanded 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 that is undergoing authentication.
- Shelf-slot NAS-Port format—This 16-bit NAS-Port format supports expanded hardware models requiring shelf and slot entries.
- PPP extended NAS-Port format—This NAS-Port format uses 32 bits to indicate the interface.



Note

This command replaces the **radius-server attribute nas-port extended** command.

Examples

In the following example, a RADIUS server is identified, and the NAS-Port field is set to the PPP extended format:

```
radius-server host 172.31.5.96 auth-port 1645 acct-port 1646
radius-server attribute nas-port format d
```

Related Commands

Command	Description
vpdn aaa attribute	Enables reporting of NAS AAA attributes related to a VPDN to the AAA server.

radius-server configure-nas

To have the Cisco router or access server query the vendor-proprietary RADIUS server for the static routes and IP pool definitions used throughout its domain when the device starts up, use the **radius-server configure-nas** global configuration command.

radius-server configure-nas

Syntax Description This command has no arguments or keywords.

Defaults None

Command Modes Global configuration

Command History	Release	Modification
	11.3	This command was introduced.

Usage Guidelines Use the **radius-server configure-nas** command to have the Cisco router query the vendor-proprietary RADIUS server for static routes and IP pool definitions when the router first starts up. 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. As each network access server starts up, it queries the RADIUS server for static route and IP pool information. This command enables the Cisco router to obtain static routes and IP pool definition information from the RADIUS server.



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

Examples The following example shows how to tell the Cisco router or access server to query the vendor-proprietary RADIUS server for already-defined static routes and IP pool definitions when the device first starts up:

```
radius-server configure-nas
```

Related Commands	Command	Description
	radius-server host non-standard	Identifies that the security server is using a vendor-proprietary implementation of RADIUS.

radius-server deadtime

To improve RADIUS response times when some servers might be unavailable, use the **radius-server deadtime** global configuration command to cause the unavailable servers to be skipped immediately. Use the **no** form of this command to set dead-time to 0.

radius-server deadtime *minutes*

no radius-server deadtime

Syntax Description	<i>minutes</i>	Length of time a RADIUS server is skipped over by transaction requests, up to a maximum of 1440 minutes (24 hours).
---------------------------	----------------	---

Defaults	Dead time is set to 0.
-----------------	------------------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	11.1	This command was introduced.

Usage Guidelines	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 <i>minutes</i> or unless there are no servers not marked “dead.”
-------------------------	---

Examples	The following example specifies five minutes dead-time for RADIUS servers that fail to respond to authentication requests:
-----------------	--

```
radius-server deadtime 5
```

Related Commands	Command	Description
	radius-server host	Specifies a RADIUS server host.
	radius-server retransmit	Specifies the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
	radius-server timeout	Sets the interval a router waits for a server host to reply.

radius-server extended-portnames

The **radius-server extended-portnames** command is replaced by the **radius-server attribute nas-port extended** command. See the description of the **radius-server attribute nas-port extended** command in this chapter for more information.

radius-server host

To specify a RADIUS server host, use the **radius-server host** global configuration command. Use the **no** form of this command to delete the specified RADIUS host.

```
radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number]
[timeout seconds] [retransmit retries] [key string]
```

```
no radius-server host {hostname | ip-address}
```

Syntax Description

<i>hostname</i>	DNS name of the RADIUS server host.
<i>ip-address</i>	IP address of the RADIUS server host.
auth-port	(Optional) Specifies the UDP destination port for authentication requests.
<i>port-number</i>	(Optional) Port number for authentication requests; the host is not used for authentication if set to 0. The default authorization port number is 1645.
acct-port	(Optional) Specifies the UDP destination port for accounting requests.
<i>port-number</i>	(Optional) Port number for accounting requests; the host is not used for accounting if set to 0. The default accounting port number is 1646.
timeout	(Optional) The time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the radius-server timeout command. If no timeout value is specified, the global value is used. Enter a value in the range 1 to 1000.
<i>seconds</i>	(Optional) Specifies the timeout value. Enter a value in the range 1 to 1000. If no timeout value is specified, the global value is used.
retransmit	(Optional) The number of times a RADIUS request is resent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the radius-server retransmit command.
<i>retries</i>	(Optional) Specifies the retransmit value. Enter a value in the range 1 to 100. If no retransmit value is specified, the global value is used.
key	(Optional) Specifies the authentication and encryption key used between the router and the RADIUS daemon running on this RADIUS server. This key overrides the global setting of the radius-server key command. If no key string is specified, the global value is used. 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 syntax. This is because the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.
<i>string</i>	(Optional) Specifies the authentication and encryption key for all RADIUS communications between the router and the RADIUS server. This key must match the encryption used on the RADIUS daemon. All 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 themselves are part of the key.

Defaults

No RADIUS host is specified; use global **radius-server** command values.

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
11.3(8)AA	This command was modified to add options for configuring timeout, retransmission, and key values per RADIUS server for the following platforms: Cisco AS5200, Cisco AS5300, Cisco AS5800, and Cisco 7200.

Usage Guidelines

You can use multiple **radius-server host** commands to specify multiple hosts. The software searches for hosts in the order you specify them.

If no host specific timeout, retransmit, or key values are specified, the global values apply to that host.

For a list of supported vendor-specific RADIUS attributes, refer to the "RADIUS Attributes" appendix in the *Security Configuration Guide*.

Examples

The following example specifies *host1* as the RADIUS server and uses default ports for both accounting and authentication:

```
radius-server host host1
```

The following example specifies port 1612 as the destination port for authentication requests and port 1616 as the destination port for accounting requests on a RADIUS host named *host1*:

```
radius-server host host1 auth-port 1612 acct-port 1616
```

Because entering a line resets all the port numbers, you must specify a host and configure accounting and authentication ports on a single line.

The following example specifies the host with IP address 172.29.39.46 as the RADIUS server, uses ports 1612 and 1616 as the authorization and accounting ports, sets the timeout value to 6, sets the retransmit value to 5, and sets "rad123" as the encryption key, matching the key on the RADIUS server:

```
radius-server host 172.29.39.46 auth-port 1612 acct-port 1616 timeout 6 retransmit 5 key rad123
```

To use separate servers for accounting and authentication, use the zero port value as appropriate. The following example specifies that RADIUS server *host1* be used for accounting but not for authentication, and that RADIUS server *host2* be used for authentication but not for accounting:

```
radius-server host host1.domain.com auth-port 0
radius-server host host2.domain.com acct-port 0
```

Related Commands

Command	Description
aaa new-model	Configures AAA security services (authentication, authorization, and accounting) on the router or access server to support the RADIUS security protocol.
radius-server timeout	Sets the interval a router waits for a server host to reply for all RADIUS servers.
radius-server retransmit	Specifies the number of times a RADIUS request is resent to a server if that server is not responding or responding slowly.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.

radius-server host non-standard

To identify that the security server is using a vendor-proprietary implementation of RADIUS, use the **radius-server host non-standard** global configuration command. This command tells the Cisco IOS software to support nonstandard RADIUS attributes. Use the **no** form of this command to delete the specified vendor-proprietary RADIUS host.

radius-server host {*hostname* | *ip-address*} **non-standard**

no radius-server host {*hostname* | *ip-address*} **non-standard**

Syntax Description	
	<i>hostname</i> DNS name of the RADIUS server host.
	<i>ip-address</i> IP address of the RADIUS server host.

Defaults No RADIUS host is specified.

Command Modes Global configuration

Command History	Release	Modification
	11.3	This command was introduced.

Usage Guidelines The **radius-server host non-standard** command enables you to identify that the RADIUS server is using a vendor-proprietary implementation of RADIUS. Although an IETF draft standard for RADIUS specifies a method for communicating information between the network access server and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. This command enables the Cisco IOS software to support the most common vendor-proprietary RADIUS attributes. Vendor-proprietary attributes will not be supported unless you use the **radius-server host non-standard** command.

For a list of supported vendor-specific RADIUS attributes, refer to the “RADIUS Attributes” appendix in the *Security Configuration Guide*.

Examples The following example specifies a vendor-proprietary RADIUS server host named *alcatraz*:

```
radius-server host alcatraz non-standard
```

Related Commands	Command	Description
	radius-server host	Specifies a RADIUS server host.
	radius-server configure-nas	Allows the Cisco router or access server to query the vendor-proprietary RADIUS server for the static routes and IP pool definitions used throughout its domain when the device starts up.

radius-server optional passwords

To specify that the first RADIUS request to a RADIUS server be made *without* password verification, use the **radius-server optional-passwords** global configuration command. Use the **no** form of this command to restore the default.

radius-server optional-passwords

no radius-server optional-passwords

Syntax Description This command has no arguments or keywords.

Defaults Disabled

Command Modes Global configuration

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines When the user enters the login name, the login request is transmitted with the name and a zero-length password. If accepted, the login procedure completes. If the RADIUS server refuses this request, the server software prompts for a password and tries again when the user supplies a password. The RADIUS server must support authentication for users without passwords to make use of this feature.

Examples The following example configures the first login to not require RADIUS verification:

```
radius-server optional-passwords
```

radius-server key

To set the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon, use the **radius-server key** global configuration command. Use the **no** form of this command to disable the key.

radius-server key {*string*}

no radius-server key

Syntax Description

<i>string</i>	The key used to set authentication and encryption for all RADIUS communications between the router and the RADIUS server.
---------------	---

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

After enabling AAA authentication with the **aaa new-model** command, you must set the authentication and encryption key using the **radius-server key** command.



Note

Specify a RADIUS key after you issue the **aaa new-model** command.

The key entered must match the key used on the RADIUS daemon. All 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 themselves are part of the key.

Examples

The following example sets the authentication and encryption key to “dare to go”:

```
radius-server key dare to go
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication ppp	Specifies one or more AAA authentication method for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict network access to a user.
ppp	Starts an asynchronous connection using PPP.

Command	Description
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
radius-server host	Specifies a RADIUS server host.
username	Establishes a username-based authentication system, such as PPP CHAP and PAP.

radius-server retransmit

To specify the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up, use the **radius-server retransmit** global configuration command. Use the **no** form of this command to disable retransmission.

radius-server retransmit *retries*

no radius-server retransmit

Syntax Description	<i>retries</i>	Maximum number of retransmission attempts. Enter a value in the range 1 to 100. If no retransmit value is specified, the global default of 3 attempts is used.
---------------------------	----------------	---

Defaults	Three retries
-----------------	---------------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	11.1	This command was introduced.

Usage Guidelines	The Cisco IOS software tries all servers, allowing each one to time out before increasing the retransmit count.
-------------------------	---

Examples	The following example specifies a retransmit counter value of five times: <pre>radius-server retransmit 5</pre>
-----------------	--

Related Commands	Command	Description
	radius-server host	Specifies a RADIUS server host.
	radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
	radius-server timeout	Specifies the time interval that the router waits for the RADIUS server to reply before retransmitting.

radius-server timeout

To set the interval a router waits for a server host to reply, use the **radius-server timeout** global configuration command. Use the **no** form of this command to restore the default.

radius-server timeout *seconds*

no radius-server timeout

Syntax Description	<i>seconds</i>	Number that specifies the timeout interval in seconds. Enter a value in the range 1 to 1000. The default is 5 seconds.
---------------------------	----------------	--

Defaults	5 seconds
-----------------	-----------

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	11.1	This command was introduced.

Usage Guidelines	Use this command to set the number of seconds a router waits for a server host to reply before timing out.
-------------------------	--

Examples	The following example changes the interval timer to 10 seconds: <pre>radius-server timeout 10</pre>
-----------------	--

Related Commands	Command	Description
	radius-server host	Specifies a RADIUS server host.
	radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
	radius-server retransmit	Specifies the number of times the Cisco IOS software searches the last of RADIUS server hosts before giving up.

radius-server vsa send

To configure the network access server to recognize and use vendor-specific attributes, use the **radius-server vsa send** global configuration command. Use the **no** form of this command to restore the default.

radius-server vsa send [accounting | authentication]

no radius-server vsa send [accounting | authentication]

Syntax Description

accounting	(Optional) Limits the set of recognized vendor-specific attributes to only accounting attributes.
authentication	(Optional) Limits the set of recognized vendor-specific attributes to only authentication attributes.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.3T	This command was introduced.

Usage Guidelines

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 **radius-server vsa send** command enables the network access server to recognize and use both accounting and authentication vendor-specific attributes. Use the **accounting** keyword with the **radius-server vsa send** command to limit the set of recognized vendor-specific attributes to just accounting attributes. Use the **authentication** keyword with the **radius-server vsa send** command to limit the set of recognized vendor-specific attributes to just authentication attributes.

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 with the following 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)."

Examples

The following example configures the network access server to recognize and use vendor-specific accounting attributes:

```
radius-server vsa send accounting
```

Related Commands

Command	Description
aaa nas-port extended	Replaces the NAS-Port attribute with RADIUS IETF Attribute 26 and displays extended field information.

vpdn aaa attribute

To enable reporting of network access server (NAS) authentication, authorization, and accounting (AAA) attributes related to a virtual private dialup network (VPDN) to the AAA server, use the **vpdn aaa attribute** command in global configuration mode. To disable reporting of AAA attributes related to VPDN, use the **no** form of this command.

```
vpdn aaa attribute {nas-ip-address vpdn-nas | nas-port vpdn-nas}
```

```
no vpdn aaa attribute {nas-ip-address vpdn-nas | nas-port}
```

Syntax Description

nas-ip-address vpdn-nas	Enable reporting of the VPDN NAS IP address to the AAA server.
nas-port vpdn-nas	Enable reporting of the VPDN NAS port to the AAA server.

Command Default

AAA attributes are not reported to the AAA server.

Command Modes

Global configuration

Command History

Release	Modification
11.3 NA	This command was introduced.
11.3(8.1)T	This command was integrated into Cisco IOS Release 11.3(8.1)T.

Usage Guidelines

This command can be used with RADIUS or TACACS+, and is applicable only on the VPDN tunnel server.

Examples

The following example configures VPDN on a tunnel server and enables reporting of VPDN AAA attributes to the AAA server:

```
vpdn enable
vpdn-group 1
  accept-dialin
  protocol any
  virtual-template 1
!
terminate-from hostname nas1
local name ts1
!
vpdn aaa attribute nas-ip-address vpdn-nas
vpdn aaa attribute nas-port vpdn-nas
```