



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 disable this feature.

aaa nas-port extended
no aaa nas-port extended

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

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 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.

Example

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

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

Related Commands

You can use the master indexes or search online to find documentation of related commands.

radius-server vsa send

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

subinterface-name Name of the interface that RADIUS uses for all of its outgoing packets.

Default

This command has no factory-assigned default.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

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 *up* 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.

Example

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

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

Related Commands

You can use the master indexes or search online to find documentation of related commands.

```
ip tacacs source-interface  
ip telnet source-interface  
ip tftp source-interface
```

radius-server attribute nas-port extended

To display expanded interface information in the NAS-Port-Type attribute, use the **radius-server attribute nas-port extended** global configuration command. Use the **no** form of this command to disable this feature.

radius-server attribute nas-port extended
no radius-server attribute nas-port extended

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

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 “ttr” 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.

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

Example

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

```
radius-server attribute nas-port extended
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

aaa nas-port extended

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.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

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 running-config startup-config** command.

Example

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

You can use the master indexes or search online to find documentation of related commands.

radius-server host non-standard

radius-server deadtime-time

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).
----------------	---

Default

Dead time is set to 0.

Command Mode

Global configuration

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 *minutes* or unless there are no servers not marked “dead.”

Example

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

```
radius-server deadtime 5
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

radius-server host
radius-server retransmit
radius-server timeout

radius-server extended-portnames

To display expanded interface information in the NAS-Port-Type attribute, use the **radius-server extended-portnames** global configuration command. Use the **no** form of this command to disable this feature.

radius-server extended-portnames
no radius-server extended-portnames

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

Note This command has been replaced by the **radius-server attribute nas-port** extended command.

Example

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

```
radius-server extended-portnames
```

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]  
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.
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.

Default

No RADIUS host is specified.

Command Mode

Global configuration

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.

Example

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

```
radius-server host host1.company.com
```

The following example specifies port 12 as the destination port for authentication requests and port 16 as the destination port for accounting requests on a RADIUS host named *host1*:

```
radius-server host host1.company.com auth-port 12 acct-port 16
```

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

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

Related Commands

You can use the master indexes or search online to find documentation of related commands.

- aaa accounting**
- aaa authentication**
- aaa authorization**
- login authentication**
- login tacacs**
- ppp**
- ppp authentication**
- radius-server key**
- slip**
- tacacs-server**
- username**

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 non-standard 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.

Default

No RADIUS host is specified.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

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*.

Example

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

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

Related Commands

You can use the master indexes or search online to find documentation of related commands.

radius-server host
radius-server configure-nas

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. This key must match the encryption used on the RADIUS daemon.
---------------	---

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

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.

Example

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

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

Related Commands

You can use the master indexes or search online to find documentation of related commands.

login authentication

login tacacs

ppp

ppp authentication

radius-server host

slip

tacacs-server

username

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

retries Maximum number of retransmission attempts. The default is 3 attempts.

Default

Three retries

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

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

Example

The following example specifies a retransmit counter value of five times:

```
radius-server retransmit 5
```

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. The default is 5 seconds.
----------------	--

Default

5 seconds

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

Example

The following example changes the interval timer to 10 seconds:

```
radius-server timeout 10
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

login authentication
login tacacs
ppp
ppp authentication
slip
tacacs-server
username

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

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3T.

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 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).”

Example

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

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

Related Commands

You can use the master indexes or search online to find documentation of related commands.

aaa nas-port extended