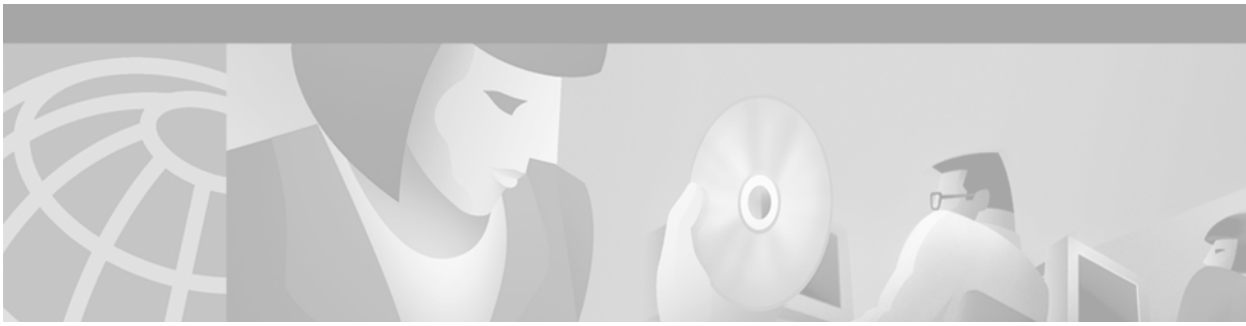

RADIUS Commands

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 chapter "Configuring RADIUS" in the *Cisco IOS Security Configuration Guide*. For configuration examples using the commands in this chapter, refer to the section "RADIUS Configuration Examples" located at the end of the chapter "Configuring RADIUS" in the *Cisco IOS Security Configuration Guide*.

aaa group server radius

To group different RADIUS server hosts into distinct lists and distinct methods, enter the **aaa group server radius** command in global configuration mode. To remove a group server from the configuration list, enter the **no** form of this command.

aaa group server radius *group-name*

no aaa group server radius *group-name*

Syntax Description

group-name	Character string used to name the group of servers.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

The authentication, authorization, and accounting (AAA) server-group feature introduces a way to group existing server hosts. The feature enables you to select a subset of the configured server hosts and use them for a particular service.

A group server is a list of server hosts of a particular type. Currently supported server host types are RADIUS server hosts and TACACS+ server hosts. A group server is used in conjunction with a global server host list. The group server lists the IP addresses of the selected server hosts.

Examples

The following example shows the configuration of an AAA group server named radgroup1 that comprises three member servers:

```
aaa group server radius radgroup1
    server 1.1.1.1 auth-port 1700 acct-port 1701
    server 2.2.2.2 auth-port 1702 acct-port 1703
    server 3.3.3.3 auth-port 1705 acct-port 1706
```

Note If auth-port and acct-port are not specified, the default value of auth-port is 1645 and the default value of acct-port is 1646.

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication login	Set AAA authentication at login.

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.

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** command in global configuration mode. To display no extended field information, use the **no** form of this command.

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 due to 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** 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.

call guard-timer

To set a guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request, use the **call guard-timer** controller configuration command. To remove the **call guard-timer** command from your configuration file, use the **no** form of this command.

call guard-timer *milliseconds* [**on-expiry** {**accept** | **reject**}]

no call guard-timer *milliseconds* [**on-expiry** {**accept** | **reject**}]

Syntax Description

milliseconds	Specifies the number of milliseconds to wait for a response from the RADIUS server.
on-expiry accept	(Optional) Accepts the call if a response is not received from the RADIUS server within the specified time.
on-expiry reject	(Optional) Rejects the call if a response is not received from the RADIUS server within the specified time.

Defaults

No default behavior or values.

Command Modes

Controller configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Examples

The following example shows a guard timer that is set at 20000 milliseconds. A call will be accepted if the RADIUS server has not responded to a preauthentication request when the timer expires.

```
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 ds0-group 0 timeslots 1-24 type e&m-fgb dtmf dnis
 cas-custom 0
    call guard-timer 20000 on-expiry accept

aaa preauth
group radius
    dnis required
```

Related Commands

Command	Description
aaa preauth	Enters AAA preauthentication configuration mode.

clid

To preauthenticate calls on the basis of the Calling Line Identification (CLID) number, use the **clid** authentication, authorization, and accounting (AAA) preauthentication configuration command. To remove the **clid** command from your configuration, use the **no** form of this command.

clid [**if-avail | required**] [**accept-stop**] [**password** *password*]

no clid [**if-avail | required**] [**accept-stop**] [**password** *password*]

Syntax Description

if-avail	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.
required	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.
accept-stop	(Optional) Prevents subsequent preauthentication elements such as **ctype** or **dnis** from being tried once preauthentication has succeeded for a call element.
password *password*	(Optional) Defines the password for the preauthentication element.

Defaults

The **if-avail** and **required** keywords are mutually exclusive. If the **if-avail** keyword is not configured, the preauthentication setting defaults to **required**.

The default password string is cisco.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You may configure more than one of the AAA preauthentication commands (**clid**, **ctype**, **dnis**) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure **dnis**, then **clid**, then **ctype**, in this order, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

Examples

The following example specifies that incoming calls be preauthenticated on the basis of the CLID number:

```
aaa preauth
 group radius
```

```
clid required
```

Related Commands

Command	Description
ctype	Preauthenticates calls on the basis of the call type.
dnis (AAA preauthentication configuration)	Preauthenticates calls on the basis of the DNIS number.
dnis bypass (AAA preauthentication configuration)	Specifies a group of DNIS numbers that will be bypassed for preauthentication.
group (AAA preauthentication configuration)	Specifies the AAA RADIUS server group to use for preauthentication.

ctype

To preauthenticate calls on the basis of the call type, use the **ctype** authentication, authorization, and accounting (AAA) preauthentication configuration command. To remove the **ctype** command from your configuration, use the **no** form of this command.

ctype [**if-avail** | **required**] [**accept-stop**] [**password** *password*] [**digital** | **speech** | **v.110** | **v.120**]

no ctype [**if-avail** | **required**] [**accept-stop**] [**password** *password*] [**digital** | **speech** | **v.110** | **v.120**]

Syntax Description

if-avail	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.
required	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.
accept-stop	(Optional) Prevents subsequent preauthentication elements such as **clid** or **dnis** from being tried once preauthentication has succeeded for a call element.
password *password*	(Optional) Defines the password for the preauthentication element.
digital	(Optional) Specifies “digital” as the call type for preauthentication.
speech	(Optional) Specifies “speech” as the call type for preauthentication.
v.110	(Optional) Specifies “v.110” as the call type for preauthentication.
v.120	(Optional) Specifies “v.120” as the call type for preauthentication.

Defaults

The **if-avail** and **required** keywords are mutually exclusive. If the **if-avail** keyword is not configured, the preauthentication setting defaults to **required**.

The default password string is cisco.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You may configure more than one of the AAA preauthentication commands (**clid**, **ctype**, **dnis**) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure **dnis**, then **clid**, then **ctype**, in this order, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

Set up the RADIUS preauthentication profile with the call type string as the username and with the password that is defined in the **ctype** command as the password. Table 15 shows the call types that you may use in the preauthentication profile.

Table 15 Preauthentication Call Types

Call Type String	ISDN Bearer Capabilities
digital	Unrestricted digital, restricted digital.
speech	Speech, 3.1 kHz audio, 7 kHz audio.
v.110	Anything with V.110 user information layer.
v.120	Anything with V.120 user information layer.

Examples

The following example specifies that incoming calls be preauthenticated on the basis of the call type:

```
aaa preauth
 group radius
 ctype required
```

Related Commands

Command	Description
clid	Preauthenticates calls on the basis of the CLID number.
dnis (AAA preauthentication configuration)	Preauthenticates calls on the basis of the DNIS number.
dnis bypass (AAA preauthentication configuration)	Specifies a group of DNIS numbers that will be bypassed for preauthentication.
group (AAA preauthentication configuration)	Specifies the AAA RADIUS server group to use for preauthentication.

deadtime (server-group configuration)

To configure deadtime within the context of RADIUS server groups, use the **deadtime** server group configuration command. To set deadtime to 0, use the **no** form of this command.

deadtime *minutes*

no deadtime

Syntax Description

minutes	Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests, up to a maximum of 1440 minutes (24 hours).

Defaults

Deadtime is set to 0.

Command Modes

Server-group configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

Use this command to configure the deadtime value of any RADIUS server group. The value of deadtime set in the server groups will override the server that is configured globally. If deadtime is omitted from the server group configuration, the value will be inherited from the master list. If the server group is not configured, the default value (0) will apply to all servers in the group.

Examples

The following example specifies a one-minute deadtime for RADIUS server group group1 once it has failed to respond to authentication requests:

```
aaa group server radius group1
    server 1.1.1.1 auth-port 1645 acct-port 1646
    server 2.2.2.2 auth-port 2000 acct-port 2001
    deadtime 1
```

Related Commands

Command	Description
radius-server deadtime	Sets the deadtime value globally.

dialer aaa

To allow a dialer to access the authentication, authorization, and accounting (AAA) server for dialing information, use the **dialer aaa** command in interface configuration mode. To disable this function, use the **no** form of this command.

dialer aaa [**password** *string* | **suffix** *string*]

no dialer aaa [**password** *string* | **suffix** *string*]

Syntax Description

password *string*	(Optional) Defines a nondefault password for authentication. The password string can be a maximum of 128 characters.
suffix *string*	(Optional) Defines a suffix for authentication. The suffix string can be a maximum of 64 characters.

Defaults

This feature is not enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.1(5)T	The **password** and **suffix** keywords were added.

Usage Guidelines

This command is required for large scale dial-out and Layer 2 Tunneling Protocol (L2TP) dial-out functionality. With this command, you can specify a suffix, a password, or both. If you do not specify a password, the default password will be "cisco."

Note Only IP addresses can be specified as usernames for the **dialer aaa suffix** command.

Examples

This example shows a user sending out packets from interface Dialer1 with a destination IP address of 1.1.1.1. The username in the access-request message is "1.1.1.1@ciscoDoD" and the password is "cisco."

```
interface dialer1
 dialer aaa
 dialer aaa suffix @ciscoDoD password cisco
```

Related Commands

Command	Description
accept dialout	Accepts requests to tunnel L2TP dial-out calls and creates an accept-dialout VPDN subgroup.

dialer congestion-threshold	Specifies congestion threshold in connected links.
dialer vpdn	Enables a Dialer Profile or DDR dialer to use L2TP dial-out.

dnis (AAA preauthentication configuration)

To preauthenticate calls on the basis of the DNIS (Dialed Number Identification Service) number, use the **dnis** AAA preauthentication configuration command. To remove the **dnis** command from your configuration, use the **no** form of this command.

dnis [**if-avail | required**] [**accept-stop**] [**password** *password*]

no dnis [**if-avail | required**] [**accept-stop**] [**password** *password*]

Syntax Description

if-avail	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.
required	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.
accept-stop	(Optional) Prevents subsequent preauthentication elements such as **clid** or **ctype** from being tried once preauthentication has succeeded for a call element.
password *password*	(Optional) Defines the password for the preauthentication element.

Defaults

The **if-avail** and **required** keywords are mutually exclusive. If the **if-avail** keyword is not configured, the preauthentication setting defaults to **required**.

The default password string is cisco.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You may configure more than one of the authentication, authorization, and accounting (AAA) preauthentication commands (**clid**, **ctype**, **dnis**) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure **dnis**, then **clid**, then **ctype**, in this order, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

Examples

The following example specifies that incoming calls be preauthenticated on the basis of the DNIS number:

```
aaa preauth
 group radius
 dnis required
```

Related Commands

Command	Description
clid	Preauthenticates calls on the basis of the CLID number.
ctype	Preauthenticates calls on the basis of the call type.
dnis bypass (AAA preauthentication configuration)	Specifies a group of DNIS numbers that will be bypassed for preauthentication.
group (AAA preauthentication configuration)	Specifies the AAA RADIUS server group to use for preauthentication.

dnis bypass (AAA preauthentication configuration)

To specify a group of DNIS (Dialed Number Identification Service) numbers that will be bypassed for preauthentication, use the **dnis bypass** AAA preauthentication configuration command. To remove the **dnis bypass** command from your configuration, use the **no** form of this command.

dnis bypass {*dnis-group-name*}

no dnis bypass {*dnis-group-name*}

Syntax Description

dnis-group-name	Name of the defined DNIS group.

Defaults

No DNIS numbers are bypassed for preauthentication.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

Before using this command, you must first create a DNIS group with the **dialer dnis group** command.

Examples

The following example specifies that preauthentication be performed on all DNIS numbers except for two DNIS numbers (12345 and 12346), which have been defined in the DNIS group called hawaii:

```
aaa preauth
 group radius
 dnis required
 dnis bypass hawaii

dialer dnis group hawaii
 number 12345
 number 12346
```

Related Commands

Command	Description
dialer dnis group	Creates a DNIS group.
dnis (AAA preauthentication configuration)	Preauthenticates calls on the basis of the DNIS number.

group (AAA preauthentication configuration)

To specify the authentication, authorization, and accounting (AAA) RADIUS server group to use for preauthentication, use the **group** AAA preauthentication configuration command. To remove the **group** command from your configuration, use the **no** form of this command.

group *server-group*

no group *server-group*

Syntax Description

server-group	Specifies a AAA RADIUS server group.

Defaults

No default behavior or values.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You must configure a RADIUS server group with the **aaa group server radius** command in global configuration mode before using the **group** command in AAA preauthentication configuration mode.

You must configure the **group** command before you configure any other AAA preauthentication command (**clid**, **ctype**, **dnis**, or **dnis bypass**).

Examples

The following example shows the creation of a RADIUS server group called “maestro” and then specifies that DNIS preauthentication be performed using this server group:

```
aaa group server radius maestro
 server 1.1.1.1
 server 2.2.2.2
 server 3.3.3.3

aaa preauth
 group maestro
 dnis required
```

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
clid	Preauthenticates calls on the basis of the CLID number.
ctype	Preauthenticates calls on the basis of the call type.
dnis (AAA preauthentication configuration)	Preauthenticates calls on the basis of the DNIS number.
dnis bypass (AAA preauthentication configuration)	Specifies a group of DNIS numbers that will be bypassed for preauthentication.

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** command in global configuration mode. To prevent RADIUS from using the IP address of a specified interface for all outgoing RADIUS packets, use the **no** form of this 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.

Defaults

No default behavior or values.

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 *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 an 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 32 include-in-access-req

To send RADIUS attribute 32 (NAS-Identifier) in an access-request or accounting-request, use the **radius-server attribute 32 include-in-access-req** global configuration command. To disable sending RADIUS attribute 32, use the **no** form of this command.

radius-server attribute 32 include-in-access-req [*format*]

no radius-server attribute 32 include-in-access-req

Syntax Description

format	(Optional) A string sent in attribute 32 containing an IP address (%i), a hostname (%h), or a domain name (%d).

Defaults

RADIUS attribute 32 is not sent in access-request or accounting-request packets.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1T	This command was introduced.

Usage Guidelines

Using the **radius-server attribute 32 include-in-access-req** makes it possible to identify the network access server (NAS) manufacturer to the RADIUS server by sending RADIUS attribute 32 (NAS-Identifier) in an access-request or accounting-request. If you configure the *format* argument, the string sent in attribute 32 will include an IP address, a hostname, or a domain name; otherwise, the Fully Qualified Domain Name (FQDN) is sent by default.

Examples

The following example shows a configuration that sends RADIUS attribute 32 in the access-request with the format configured to identify a Cisco NAS:

```
radius-server attribute 32 include-in-access-req format cisco %h.%d %i
! The following string will be sent in attribute 32 (NAS-Identifier).
"cisco router.nlab.cisco.com 10.0.1.67"
```

radius-server attribute 44 include-in-access-req

To send RADIUS attribute 44 (Accounting Session ID) in access request packets before user authentication (including requests for preauthentication), use the **radius-server attribute 44 include-in-access-req** global configuration command. To remove this command from your configuration, use the **no** form of this command.

radius-server attribute 44 include-in-access-req

no radius-server attribute 44 include-in-access-req

Syntax Description

This command has no arguments or keywords.

Defaults

RADIUS attribute 44 is not sent in access request packets.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.

Usage Guidelines

There is no guarantee that the Accounting Session IDs will increment uniformly and consistently. In other words, between two calls, the Accounting Session ID can increase by more than one.

Examples

The following example shows a configuration that sends RADIUS attribute 44 in access-request packets:

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 include-in-access-req
```

radius-server attribute 55 include-in-acct-req

To send the RADIUS attribute 55 (Event-Timestamp) in accounting packets, use the **radius-server attribute 55 include-in-acct-req** command in global configuration mode. To remove this command from your configuration, use the **no** form of this command.

radius-server attribute 55 include-in-acct-req

no radius-server attribute 55 include-in-acct-req

Syntax Description

This command has no arguments or keywords.

Defaults

RADIUS attribute 55 is not sent in accounting packets.

Command Modes

Global configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

Use the **radius-server attribute 55 include-in-acct-req** command to send RADIUS attribute 55 (Event-Timestamp) in accounting packets. The Event-Timestamp attribute records the time that the event occurred on the NAS; the timestamp sent in attribute 55 is in seconds since January 1, 1970 00:00 UTC.

Note Before the Event-Timestamp attribute can be sent in accounting packets, you *must* configure the clock on the router. (For information on setting the clock on your router, refer to section "Performing Basic System Management" in the chapter "System Management" of the *Cisco IOS Configuration Fundamentals Configuration Guide*.)

To avoid configuring the clock on the router every time the router is reloaded, you can enable the **clock calendar-valid** command. (For information on this command, refer to the chapter "Basic System Management Commands" in the *Cisco IOS Configuration Fundamentals Command Reference.*

Examples

The following example shows how to enable your router to send the Event-Timestamp attribute in accounting packets. (To see whether the Event-Timestamp was successfully enabled, use the **debug radius** command.)

```
radius-server attribute 55 include-in-acct-req
```

Related Commands

Command	Description
clock calendar-valid	Configures a system as an authoritative time source for a network based on its hardware clock (calendar).
clock set	Manually sets the system software clock.

radius-server attribute 69 clear

To receive nonencrypted tunnel passwords in attribute 69 (Tunnel-Password), use the **radius-server attribute 69 clear** global configuration command. To disable this feature and receive encrypted tunnel passwords, use the **no** form of this command.

radius-server attribute 69 clear

no radius-server attribute 69 clear

Syntax Description

This command has no arguments or keywords.

Defaults

RADIUS attribute 69 is not sent and encrypted tunnel passwords are sent.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1(5)T	This command was introduced.

Usage Guidelines

Use the **radius-server attribute 69 clear** command to receive nonencrypted tunnel passwords, which are sent in RADIUS attribute 69 (Tunnel-Password). This command allows tunnel passwords to be sent in a "string" encapsulated format, rather than the standard tag/salt/string format, which enables the encrypted tunnel password.

Some RADIUS servers do not encrypt Tunnel-Password; however the current NAS (network access server) implementation will decrypt a non-encrypted password that causes authorization failures. Because nonencrypted tunnel passwords can be sent in attribute 69, the NAS will no longer decrypt tunnel passwords.

Note Once this command is enabled, all tunnel passwords received will be nonencrypted until the command is manually disabled.

Examples

The following example shows how to enable attribute 69 to receive nonencrypted tunnel passwords. (To see whether the Tunnel-Password process is successful, use the **debug radius** command.)

```
radius-server attribute 69 clear
```

radius-server attribute 188 format non-standard

To send the number of remaining links in the multilink bundle in the accounting-request packet, use the **radius-server attribute 188 format non-standard** global configuration command. To disable the sending of the number of links in the multilink bundle in the accounting-request packet, use the **no** form of this command.

radius-server attribute 188 format non-standard

no radius-server attribute 188 format non-standard

Syntax Description

This command has no arguments or keywords.

Defaults

RADIUS attribute 188 is not sent in accounting "start" and "stop" records.

Command Modes

Global configuration mode

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

Use this command to send attribute 188 in accounting "start" and "stop" records.

Examples

The following example shows a configuration that sends RADIUS attribute 188 in accounting-request packets:

```
radius-server attribute 188 format non-standard
```

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

format	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.
12.1(5)T	The PPP extended NAS-Port format was expanded to support PPPoE over ATM and PPPoE over IEEE 802.1Q VLANs.

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, VPI, and VCI for PPP over ATM and PPPoE over ATM, and the interface and VLAN ID for PPPoE over IEEE 802.1Q VLANs.

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 challenge-noecho

To prevent user responses to Access-Challenge packets from being displayed on the screen, use the **radius-server challenge-noecho** global configuration command. To return to the default condition, use the **no** form of this command.

radius-server challenge-noecho

no radius-server challenge-noecho

Syntax Description

This command has no arguments or keywords.

Defaults

All user responses to Access-Challenge packets are echoed to the screen.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

This command applies to all users. When the **radius-server challenge-noecho** command is configured, user responses to Access-Challenge packets are not displayed unless the Prompt attribute in the user profile is set to *echo* on the RADIUS server. The Prompt attribute in a user profile overrides the **radius-server challenge-noecho** command for the individual user. For more information, see the chapter "Configuring RADIUS" in the *Cisco IOS Security Configuration Guide*, Release 12.2.

Examples

The following example stops all user responses from displaying on the screen:

```
radius-server challenge-noecho
```

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** command in global configuration mode. To discontinue the query of the RADIUS server, use the **no** form of this command.

radius-server configure-nas

no radius-server configure-nas

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

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** command in global configuration mode to cause the unavailable servers to be skipped immediately. To set dead-time to 0, use the **no** form of this command.

radius-server deadtime *minutes*

no radius-server deadtime

Syntax Description

minutes	Length of time, in minutes, for which 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 *minutes* or unless there are no servers not marked "dead."

Examples

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

```
radius-server deadtime 5
```

Related Commands

Command	Description
deadtime (server-group configuration)	Configures deadtime within the context of RADIUS server groups.
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 for which a router waits for a server host to reply.

radius-server directed-request

To allow users logging into a Cisco netword access server (NAS) to select a RADIUS server for authentication, use the **radius-server directed-request** command in global configuration mode. To disable the directed-request feature, use the **no** form of this command.

radius-server directed-request [**restricted**]

no radius-server directed-request [**restricted**]

Syntax Description

restricted	(Optional) Prevents the user from being sent to a secondary server if the specified server is not available.

Defaults

User cannot log into a Cisco NAS to select a RADIUS server for authentication.

Command Modes

Global configuration mode

Command History

Release	Modification
12.0(2)T	This command was introduced.

Usage Guidelines

The **radius-server directed-request** command sends only the portion of the username before the "@" symbol to the host specified after the "@" symbol. In other words, with this command enabled, you can direct a request to any of the configured servers, and only the username is sent to the specified server.

Disabling the **radius-server directed-request** command causes the whole string, both before and after the "@" symbol, to be sent to the default RADIUS server. The router queries the list of servers, starting with the first one in the list. It sends the whole string, and accepts the first response that it gets from the server.

Use the **radius-server directed-request restricted** command to limit the user to the RADIUS server identified as part of the username.

The **no radius-server directed-request** command causes the entire username string to be passed to the default RADIUS server.

Note When **no radius-server directed-request restricted** is entered, only the "restricted" flag is removed, and the "directed-request" flag is retained. To disable the directed-request feature, you must also issue the **no radius-server directed-request** command.

Examples

The following example verifies that the RADIUS server is selected based on the directed request:

```
aaa new-model
aaa authentication login default radius
radius-server host 192.168.1.1
radius-server host 172.16.56.103
```

```
radius-server host 172.31.40.1
radius-server directed-request
```

radius-server extended-portnames

The **radius-server extended-portnames** 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 host

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

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

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

Syntax Description

hostname	Domain Name System (DNS) name of the RADIUS server host.
ip-address	IP address of the RADIUS server host.
auth-port	(Optional) Specifies the UDP destination port for authentication requests.
port-number	(Optional) Port number for authentication requests; the host is not used for authentication if set to 0. If unspecified, the port number defaults to 1645.
acct-port	(Optional) Specifies the UDP destination port for accounting requests.
port-number	(Optional) Port number for accounting requests; the host is not used for accounting if set to 0. If unspecified, the port number defaults to 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.
seconds	(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 re-sent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the **radius-server retransmit** command.
retries	(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.
string	(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.
alias	(Optional) Allows up to eight aliases per line for any given RADIUS server.

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.
12.0(5)T	This command was modified to add options for configuring timeout, retransmission, and key values per RADIUS server.
12.1(3)T	The **alias** keyword was added on the Cisco AS5300 and AS5800 universal access servers.

Usage Guidelines

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

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

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

The following example specifies four aliases on the RADIUS server with IP address 172.1.1.1:

```
radius-server host 172.1.1.1 acct-port 1645 auth-port 1646
radius-server host 172.1.1.1 alias 172.16.2.1 172.17.3.1 172.16.4.1
```

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.
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 key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server retransmit	Specifies how many 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.
username	Establishes a username-based authentication system, such as PPP CHAP and PAP.

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** command in global configuration mode. This command tells the Cisco IOS software to support nonstandard RADIUS attributes. To delete the specified vendor-proprietary RADIUS host, use the **no** form of this command.

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

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

Syntax Description

hostname	DNS name of the RADIUS server host.
ip-address	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 appendix "RADIUS Attributes" in the *Cisco IOS 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 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 host	Specifies a RADIUS server host.

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** command in global configuration mode. To disable the key, use the **no** form of this command.

radius-server key {**0** *string* | **7** *string* | *string*}

no radius-server key

Syntax Description

0	Specifies that an unencrypted key will follow.
string	The unencrypted (cleartext) shared key.
7	Specifies that a hidden key will follow.
string	The hidden shared key.
string	The unencrypted (cleartext) shared key.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.1(3)T	The *string* argument was modified as follows: • **0** *string* • **7** *string* • *string*

Usage Guidelines

After enabling authentication, authorization, and accounting (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
```

The following example sets the authentication and encryption key to "anykey." The 7 specifies that a hidden key will follow.

```
service password-encryption
radius-server key 7 anykey
```

After you save your configuration and use the **show-running config** command, an encrypted key will be displayed as follows:

```
show running-config
!
!
  radius-server key 7 19283103834782sda
!The leading 7 indicates that the following text is encrypted.
```

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 methods for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict user access to a network.
ppp	Starts an asynchronous connection using PPP.
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.
service password-encryption	Encrypt passwords.
username	Establishes a username-based authentication system, such as PPP CHAP and PAP.

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** command in global configuration mode. To restore the default, use the **no** form of this command.

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 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** command in global configuration mode. To disable retransmission, use the **no** form of this command.

radius-server retransmit *retries*

no radius-server retransmit

Syntax Description

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

Defaults

3 attempts

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:

```
radius-server retransmit 5
```

radius-server timeout

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

radius-server timeout *seconds*

no radius-server timeout

Syntax Description

seconds	Number that specifies the timeout interval, in seconds. 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:

```
radius-server timeout 10
```

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 unique-ident

To assign a unique accounting session identification (Acct-Session-Id), use the **radius-server unique-ident** command in global configuration mode. To disable this command, use the **no** form of this command.

radius-server unique-ident *number*

no radius-server unique-ident *number+1*

Syntax Description

number	Acct-Session-Id string.

Defaults

This command is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2	This command was introduced.

Usage Guidelines

Use the **radius-server unique-ident** command to ensure that RADIUS Acct-Session-IDs are unique across Cisco IOS boots. After the router parses this command, **radius-server unique-ident** *n+1* is written to RAM; thereafter, the Acct-Session-ID attribute will have its higher order eight bits set to n+1 in all accounting records.

After the router is reloaded, it will parse the **radius-server unique-ident** *n+1* command, and the **radius-server unique-ident** *n+2* will be written to NVRAM. Thus, the Cisco IOS configuration is automatically written to NVRAM after the router reboots.

Note **radius-server unique-ident** *255* has the same functionality as **radius-server unique-ident** 0; thus, **radius-server unique-ident** *1* is written to NVRAM when either number (255 or 0) is used.

Examples

The following example shows how to define the Acct-Session-Id to 1. In this example, the Acct-Session-ID begins as "acct-session-id = 01000008," but after enabling this command and rebooting the router, the Acct-Session-ID becomes "acct-session-id = 02000008" because the value increments by one and is updated in the system configuration.

```
radius-server unique-ident 1
```

radius-server vsa send

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

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.

server (RADIUS)

To configure the IP address of the RADIUS server for the group server, use the **server** command in server-group configuration mode. To remove the associated server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

server *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]

no server *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]

Syntax Description

ip-address	IP address of the RADIUS server host.
auth-port *port-number*	(Optional) Specifies the User Datagram Protocol (UDP) destination port for authentication requests. The port-number argument specifies the port number for authentication requests. The host is not used for authentication if this value is set to 0.
acct-port *port-number*	(Optional) Specifies the UDP destination port for accounting requests. The port number argument specifies the port number for accounting requests. The host is not used for accounting services if this value is set to 0.

Defaults

If no port attributes are defined, the defaults are as follows:

- Authentication port: 1645
- Accounting port: 1646

Command Modes

Server-group configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(7)T	The following new keywords/arguments were added: • **auth-port** *port-number* • **acct-port** *port-number*

Usage Guidelines

Use the **server** command to associate a particular server with a defined group server. There are two different ways in which you can identify a server, depending on the way you want to offer AAA services. You can identify the server simply by using its IP address, or you can identify multiple host instances or entries using the optional **auth-port** and **acct-port** keywords.

When you use the optional keywords, the network access server identifies RADIUS security servers and host instances associated with a group server on the basis of their IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS host entries providing a specific AAA service. If two different host entries on the same RADIUS server are configured for the same service—for example, accounting—the second host entry configured acts as failover backup to the first one. Using this

example, if the first host entry fails to provide accounting services, the network access server will try the second host entry configured on the same device for accounting services. (The RADIUS host entries will be tried in the order they are configured.)

Examples

Configuring Multiple Entries for the Same Server IP Address

The following example shows the network access server configured to recognize several RADIUS host entries with the same IP address. Two different host entries on the same RADIUS server are configured for the same services—authentication and accounting. The second host entry configured acts as fail-over backup to the first one. (The RADIUS host entries are tried in the order in which they are configured.)

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default radius
! The next set of commands configures multiple host entries for the same IP address.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.20.0.1 auth-port 2000 acct-port 2000
```

Configuring Multiple Entries Using AAA Group Servers

In this example, the network access server is configured to recognize two different RADIUS group servers. One of these groups, group1, has two different host entries on the same RADIUS server configured for the same services. The second host entry configured acts as failover backup to the first one.

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default group group1
! The following commands define the group1 RADIUS group server and associates servers
! with it.
aaa group server radius group1
   server 172.20.0.1 auth-port 1000 acct-port 1001
! The following commands define the group2 RADIUS group server and associates servers
! with it.
aaa group server radius group2
   server 172.20.0.1 auth-port 2000 acct-port 2001
! The following set of commands configures the RADIUS attributes for each host entry
! associated with one of the defined group servers.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
```

Related Commands

Command	Description
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.

show radius statistics

To display the RADIUS statistics for accounting and authentication packets, use the **show radius statistics** EXEC command.

show radius statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced.

Examples

The following example is sample output for the **show radius statistics** command:

```
Router# show radius statistics
                                  Auth.       Acct.        Both
          Maximum inQ length:       NA          NA           1
        Maximum waitQ length:       NA          NA           1
        Maximum doneQ length:       NA          NA           1
        Total responses seen:        3           0           3
      Packets with responses:        3           0           3
   Packets without responses:        0           0           0
  Average response delay(ms):     5006           0        5006
  Maximum response delay(ms):    15008           0       15008
   Number of Radius timeouts:        3           0           3
        Duplicate ID detects:        0           0           0
```

Table 16 describes significant fields shown in the display.

Table 16 show radius statistics Field Descriptions

Auth.	Statistics for authentication packets.
Acct.	Statistics for accounting packets.
Both	Combined statistics for authentication and accounting packets.
Maximum inQ length	Maximum number of entries allowed in the queue, that holds the RADIUS messages not yet sent.
Maximum waitQ length	Maximum number of entries allowed in the queue, that holds the RADIUS messages that have been sent and are waiting for a response.
Maximum doneQ length	Maximum number of entries allowed in the queue, that holds the messages that have received a response and will be forwarded to the code that is waiting for the messages.

Table 16 show radius statistics Field Descriptions (continued)

Total responses seen	Number of RADIUS responses seen from the server. In addition to the expected packets, this includes repeated packets and packets that do not have a matching message in the waitQ.
Packets with responses	Number of packets that received a response from the RADIUS server.
Packets without responses	Number of packets that never received a response from any RADIUS server.
Average response delay	Average time from when the packet was first transmitted to when it received a response. If the response timed out and the packet was sent again, this value includes the timeout. If the packet never received a response, this is not included in the average.
Maximum response delay	Maximum delay observed while gathering average response delay information.
Number of RADIUS timeouts	Number of times a server did not respond, and the RADIUS server re-sent the packet.
Duplicate ID detects	RADIUS has a maximum of 255 unique IDs. In some instances there can be more than 255 outstanding packets. When a packet is received, the doneQ is searched from the oldest entry to the youngest. If the IDs are the same, further techniques are used to see if this response matches this entry. If it is determined that this does not match, the duplicate ID detect counter is increased.

Related Commands

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

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.
12.1(5)T	This command was modified to support the PPP extended NAS-Port format.

Usage Guidelines

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

The PPP extended NAS-Port format enables the NAS-Port and NAS-Port-Type attributes to provide port details to a RADIUS server when one of the following protocols is configured:

- PPP over ATM
- PPP over Ethernet (PPPoE) over ATM
- PPPoE over 802.1Q VLANs

Before PPP extended NAS-Port format attributes can be reported to the RADIUS server, the **radius-server attribute nas-port format** command with the **d** keyword must be configured on both the tunnel server and the NAS, and the tunnel server and the NAS must both be Cisco routers.

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
```

The following example configures the tunnel server for VPDN, enables AAA, configures a RADIUS AAA server, and enables reporting of PPP extended NAS-Port format values to the RADIUS server. PPP extended NAS-Port format must also be configured on the NAS for this configuration to be effective.

```
vpdn enable
vpdn-group L2TP-tunnel
 accept-dialin
  protocol l2tp
  virtual-template 1
!
 terminate-from hostname nas1
 local name ts1
!
aaa new-model
aaa authentication ppp default local group radius
aaa authorization network default local group radius
aaa accounting network default start-stop group radius
!
radius-server host 171.79.79.76 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute nas-port format d
radius-server key ts123
!
vpdn aaa attribute nas-port vpdn-nas
```

Related Commands

Command	Description
radius-server attribute nas-port format	Selects the NAS-Port format used for RADIUS accounting features.