

radius attribute nas-port-type

To configure subinterfaces such as Ethernet, virtual LANs (VLAN), stacked VLAN (Q-in-Q), virtual circuit (VC), and VC ranges, use the **radius attribute nas-port-type** command in subinterface configuration mode. To disable the subinterface configuration, use the **no** form of this command.

radius attribute nas-port-type *port number*

no radius attribute nas-port-type *port number*

Syntax Description

<i>value</i>	Number assigned for a port type. <ul style="list-style-type: none"> The <i>port number</i> must be assigned a number 1–40 to set a customized extended NAS-Port Type and configure a specific service port type. <p>Choosing a number outside of this range will force the default NAS port format e string to be used to configure the value for attribute 5 that is sent for that session.</p> <ul style="list-style-type: none"> You can set a specific service port type with the radius-server attribute nas-port format command. <p>Note This setting will override a global NAS-Port-Type session format.</p>
--------------	--

Defaults

NAS-Port-Type is not configured.

Command Modes

Subinterface configuration

Command History

Release	Modification
12.3(7)XI	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

You can override the attribute 61 configured globally at a subinterface level.

To set a different extended attribute 61 value for a subinterface, such as for Ethernet, VLAN, Q-in-Q, VC, or VC ranges, select a value for that port type. An extended attribute 61 setting at a subinterface level will override the global extended attribute 61 value.

Examples

The following example shows how to override the global value set for an extended attribute 61 by setting a separate value of type 30 (PPP over ATM [PPPoA]) on a specific ATM subinterface:

```
Router# configure terminal
Router(config)#
Router(config)# interface atm 5/0/0.1
Router(config-subif)# pvc 1/33
```

```
Router(config-if-atm-vc)#  
Router(config-if-atm-vc)# radius attribute nas-port-type 30
```

Related Commands

Command	Description
radius-server attribute 61 extended	Enables extended, non-RFC-compliant NAS-Port-Type attribute (RADIUS attribute 61).
radius-server attribute nas-port format	Sets the NAS-Port format used for RADIUS accounting features and restores the default NAS-Port format, or sets the global attribute 61 session format e string or configures a specific service port type for attribute 61 support.

radius-server accounting system host-config

To enable the router to send a system accounting record for the addition and deletion of a RADIUS server, use the **radius-server accounting system host-config** command in global configuration mode.

To to disable system accounting records, use the **no** form of this command:

```
radius-server accounting system host-config
```

```
no radius-server accounting system host-config
```

Command Default

The command-level default is not enabled.

Command Modes

Global configuration mode (config)

Command History

Release	Modification
12.4	This command was introduced in Cisco IOS Release 12.4.

Usage Guidelines

The **radius-server accounting system host-config** command is used when configuring RADIUS system accounting on the global RADIUS server.

Examples

The following example shows how RADIUS system accounting is configured with the **radius-server accounting system host-config** command to enable system accounting records on a RADIUS server and private server hosts when they are added or deleted:

```
Router> enable
Router# configure terminal
Router(config)# aaa new-model
Router(config)# radius-server accounting system host-config
Router(config)# aaa group server radius radgroup1
Router(config-sg-radius)# server-private 172.16.1.11 key cisco
Router(config-sg-radius)# accounting system host-config
```

Related Commands

Command	Description
aaa new-model	Enables AAA network security services.
aaa group server radius	Adds the RADIUS server
server-private	Enters the hostname or IP address of the RADIUS server and hidden server key.
accounting system host-config	Enables the generation of system accounting records for private server hosts when they are added or deleted.

radius-server attribute 11 direction default

To specify the default direction of filters from RADIUS, use the **radius-server attribute 11 direction default** command in global configuration mode. To remove this functionality from your configuration, use the **no** form of this command.

radius-server attribute 11 direction default [inbound | outbound]

no radius-server attribute 11 direction default [inbound | outbound]

Syntax Description

inbound	(Optional) Filtering is applied to inbound packets only.
outbound	(Optional) Filtering is applied to outbound packets only.

Command Default

If this command is not enabled, filters are treated as outbound.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2(31)SB3	This feature was integrated into Cisco IOS Release 12.2(31)SB3.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **radius-server attribute 11 direction default** command to change the default direction of filters from RADIUS (RADIUS attribute 11 (Filter-Id) indicates the name of the filter list for the user). Enabling this command allows you to change the filter direction to inbound—which stops traffic from entering a router and prevents resource consumption—rather than keeping the outbound default direction, where filtering occurs only as the traffic is about to leave the network.

Examples

The following example shows how to configure RADIUS attribute 11 to change the default direction of filters. In this example, the filtering is applied to inbound packets only.

```
radius-server attribute 11 direction default inbound
```

The following is an example of a RADIUS user profile (Merit Daemon format) that includes RADIUS attribute 11 (Filter-Id):

```
client Password = "password1"
    Service-Type = Framed,
    Framed-Protocol = PPP,
    Filter-Id = "myfilter.out"
```

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** command in global configuration mode. 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

Command History	Release	Modification
	12.1	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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 31

To configure Calling-Station-Id (attribute 31) options, use the **radius-server attribute 31** command in global configuration mode. To disable the Calling-Station-Id (attribute 31) options, use the **no** form of this command.

```
radius-server attribute 31 { mac format { default | ietf | unformatted } | remote-id | send
nas-port-detail [mac-only]}
```

```
no radius-server attribute 31 { mac format { default | ietf | unformatted } | remote-id | send
nas-port-detail [mac-only]}
```

Syntax Description		
mac format	Specifies the format of the MAC address in the Calling Station ID. Select one of the following three options:	<ul style="list-style-type: none"> default (Example: 0000.4096.3e4a) ietf (Example: 00-00-40-96-3E-4A) unformatted (Example: 000040963e4a)
remote-id	Sends the remote ID as the Calling Station ID in the accounting records and access requests.	
send nas-port-detail	Includes all NAS port details in the Calling Station ID.	
mac-only	(Optional) Includes the MAC-address only, if available, in the Calling Station ID.	

Command Default The Calling-Station-Id (attribute 31) is not sent.

Command Modes Global configuration

Command History	Release	Modification
	12.2(28)SB	This command was introduced.
	12.2(31)SB2	The mac format default , the mac format ietf , the mac format unformatted , and the send nas-port-detail [mac-only] keyword options were added.
	12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

- For PPP over Ethernet over ATM (PPPoEoA) sessions:

When the **send nas-port-detail** keyword and the **mac-only** option are configured, the Calling-Station-Id (attribute 31) information is sent in Access and Accounting requests in the following format:

```
host.domain:vp_descr:vpi:vci
```

- For PPP over Ethernet over Ethernet (PPPoEoE) sessions:

When the **send nas-port-detail** keyword and the **mac-only** option are configured, the Calling-Station-Id (attribute 31) information is sent in Access and Accounting requests in the following format:

```
mac_addr
```

- For PPP over ATM sessions:

When the **send nas-port-detail** keyword and the **mac-only** option are configured, the Calling-Station-Id (attribute 31) information is sent in Access and Accounting requests in the following format:

```
host.domain:vp_descr:vpi:vci
```

Examples

The following example specifies the MAC address in the Calling Station ID to be displayed in IETF format:

```
Router(config)# radius-server attribute 31 mac format ietf
```

The following example allows the remote ID to be sent as the Calling Station ID:

```
Router(config)# radius-server attribute 31 remote-id
```

The following example allows the NAS port details to be included in the Calling Station ID:

```
Router(config)# radius-server attribute 31 send nas-port-detail
```

The following example allows only the MAC address, if available, to be included in the Calling Station ID:

```
Router(config)# radius-server attribute 31 send nas-port-detail mac-only
```

radius-server attribute 31 mac format

To configure a nondefault MAC address format in the calling line ID (CLID) of a DHCP accounting packet, use the **radius-server attribute 31 mac format** command in global configuration mode. To set the format back to the default MAC address format, use the **no** form of this command.

```
radius-server attribute 31 mac format { default | ietf | unformatted }
```

```
no radius-server attribute 31 mac format { default | ietf | unformatted }
```

Syntax Description

default	Sets the MAC address format to the default format (for example, aaaa.bbbb.cccc)
ietf	Internet Engineering Task Force (IETF) format (for example, aa-aa-bb-bb-cc-cc).
unformatted	Unformatted raw MAC address (for example, aaaabbbbcccc).

Command Default

If not configured, the format is set to the default format.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2S, 12.3	This command was introduced.

Usage Guidelines

The CLID (attribute 31) is used to carry a variety of information, such as phone numbers, IP addresses, and MAC addresses.



Note

The **radius-server attribute 31 send nas-port-detail mac-only** command must also be configured or the CLID will not be sent in the request even if the **radius-server attribute 31 mac format** command is configured.

Examples

The following example shows that the RADIUS calling station ID has been set to “unformatted”:

```
Router# radius-server attribute 31 mac format unformatted
```

Related Commands

Command	Description
radius-server attribute 31 send nas-port-detail mac-only	Configures Calling-Station-ID (attribute 31) options.

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** command in global configuration mode. 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

Command History

Release	Modification
12.1 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Using the **radius-server attribute 32 include-in-access-req** command 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 4

To configure an IP address for the RADIUS attribute 4 address, use the **radius-server attribute 4** command in global configuration mode. To delete an IP address as the RADIUS attribute 4 address, use the **no** form of this command.

radius-server attribute 4 *ip-address*

no radius-server attribute 4 *ip-address*

Syntax Description

<i>ip-address</i>	IP address to be configured as RADIUS attribute 4 inside RADIUS packets.
-------------------	--

Defaults

If this command is not configured, the RADIUS NAS-IP-Address attribute will be the IP address on the interface that connects the network access server (NAS) to the RADIUS server.

Command Modes

Global configuration

Command History

Release	Modification
12.3(3)B	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Normally, when the **ip radius-source interface** command is configured, the IP address on the interface that is specified in the command is used as the IP address in the IP headers of the RADIUS packets and as the RADIUS attribute 4 address inside the RADIUS packets.

However, when the **radius-server attribute 4** command is configured, the IP address in the command is used as the RADIUS attribute 4 address inside the RADIUS packets. There is no impact on the IP address in the IP headers of the RADIUS packets.

If both commands are configured, the IP address that is specified in the **radius-server attribute 4** command is used as the RADIUS attribute 4 address inside the RADIUS packets. The IP address on the interface that is specified in the **ip radius-source interface** command is used as the IP address in the IP headers of the RADIUS packets.

Some authentication, authorization, and accounting (AAA) clients (such as PPP, virtual private dial-up network [VPDN] or Layer 2 Tunneling Protocol [L2TP], Voice over IP [VoIP], or Service Selection Gateway [SSG]) may try to set the RADIUS attribute 4 address using client-specific values. For example, on an L2TP network server (LNS), the IP address of the L2TP access concentrator (LAC) could be specified as the RADIUS attribute 4 address using a VPDN or L2TP command. When the **radius-server attribute 4** command is configured, the IP address specified in the command takes precedence over all IP addresses from AAA clients.

During RADIUS request retransmission and during RADIUS server failover, the specified IP address is always chosen as the value of the RADIUS attribute 4 address.

Examples

The following example shows that the IP address 10.0.0.21 has been configured as the RADIUS NAS-IP-Address attribute:

```
radius-server attribute 4 10.0.0.21
radius-server host 10.0.0.10 auth-port 1645 acct-port 1646 key cisco
```

The following **debug radius** command output shows that 10.0.0.21 has been successfully configured.

```
Router# debug radius

RADIUS/ENCODE(0000001C): acct_session_id: 29
RADIUS(0000001C): sending
RADIUS(0000001C): Send Access-Request to 10.0.0.10:1645 id 21645/17, len 81
RADIUS: authenticator D0 27 34 C0 F0 C4 1C 1B - 3C 47 08 A2 7E E1 63 2F
RADIUS: Framed-Protocol      [7] 6 PPP [1]
RADIUS: User-Name           [1] 18 "shashi@pepsi.com"
RADIUS: CHAP-Password       [3] 19 *
RADIUS: NAS-Port-Type       [61] 6 Virtual [5]
RADIUS: Service-Type        [6] 6 Framed [2]
RADIUS: NAS-IP-Address      [4] 6 10.0.0.21
UDP: sent src=11.1.1.1(21645), dst=10.0.0.10(1645), length=109
UDP: rcvd src=10.0.0.10(1645), dst=10.1.1.1(21645), length=40
RADIUS: Received from id 21645/17 10.0.0.10:1645, Access-Accept, len 32
RADIUS: authenticator C6 99 EC 1A 47 0A 5F F2 - B8 30 4A 4C FF 4B 1D F0
RADIUS: Service-Type        [6] 6 Framed [2]
RADIUS: Framed-Protocol     [7] 6 PPP [1]
RADIUS(0000001C): Received from id 21645/17
```

Related Commands

Command	Description
ip radius-source interface	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.

radius-server attribute 44 extend-with-addr

To add the accounting IP address before the existing session ID, use the **radius-server attribute 44 extend-with-addr** command in global configuration mode. To remove this command from your configuration, use the **no** form of this command.

radius-server attribute 44 extend-with-addr

no radius-server attribute 44 extend-with-addr

Syntax Description

This command has no arguments or keywords.

Defaults

This command is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The **radius-server attribute 44 extend-with-addr** command adds Acct-Session-Id (attribute 44) before the existing session ID (NAS-IP-Address).

When multiple network access servers (NAS) are being processed by one offload server, enable this command on all NASs and the offload server to ensure a common and unique session ID.



Note

This command should be enabled only when offload servers are used.

Examples

The following example shows how to configure unique session IDs among NASs:

```
aaa new-model
aaa authentication ppp default group radius
radius-server host 10.100.1.34
radius-server attribute 44 extend-with-addr
```

Related Commands

Command	Description
radius-server attribute 44 include-in-access-req	Sends RADIUS attribute 44 (Acct-Session-Id) in access-request packets before user authentication.
radius-server attribute 44 sync-with-client	Configures the offload server to synchronize accounting session information with the NAS clients.

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** command in global configuration mode. To remove this command from the configuration, use the **no** form of this command.

radius-server attribute 44 include-in-access-req [*vrf vrf-name*]

no radius-server attribute 44 include-in-access-req [*vrf vrf-name*]

Syntax Description	vrf vrf-name (Optional) Per VRF configuration.
---------------------------	---

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.
	12.2(1)DX	The vrf keyword and <i>vrf-name</i> argument were introduced on the Cisco 7200 series and Cisco 7401ASR.
	12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
	12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
	12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
	12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
	12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
	12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

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.
-------------------------	--

The **vrf vrf-name** keyword and argument specify Accounting Session IDs per Virtual Private Network (VPN) routing and forwarding (VRF), which allows multiple disjointed routing or forwarding tables, where the routes of a user have no correlation with the routes of another user.

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 44 sync-with-client

To configure the offload server to synchronize accounting session information with the network access server (NAS) clients, use the **radius-server attribute 44 sync-with-client** command in global configuration mode. To disable this functionality, use the **no** form of this command.

radius-server attribute 44 sync-with-client

no radius-server attribute 44 sync-with-client

Syntax Description This command has no arguments or keywords.

Command Default This command is not enabled.

Command Modes Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Use the **radius-server attribute 44 sync-with-client** command to allow the offload server to synchronize accounting session information with the NAS clients. The NAS-IP-Address, the Acct-Session-Id, and the Class attribute are transmitted from the client to the offload server via Layer 2 Forwarding (L2F) options.

Examples

The following example shows how to configure the offload server to synchronize accounting session information with the NAS clients:

```
radius-server attribute 44 sync-with-client
```

Related Commands

Command	Description
radius-server attribute 44 extend-with-addr	Adds the accounting IP address before the existing session ID.
radius-server attribute 44 include-in-access-req	Sends RADIUS attribute 44 (Acct-Session-Id) in access-request packets before user authentication.

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.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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 and Network Management 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 *Cisco IOS Configuration Fundamentals and Network Management 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 6

To provide for the presence of the Service-Type attribute (attribute 6) in RADIUS Access-Accept messages, use the **radius-server attribute 6** command in global configuration mode. To make the presence of the Service-Type attribute optional in Access-Accept messages, use the **no** form of this command.

radius-server attribute 6 { **mandatory** | **on-for-login-auth** | **support-multiple** | **voice** *value* }

no radius-server attribute 6 { **mandatory** | **on-for-login-auth** | **support-multiple** | **voice** *value* }

Syntax Description

mandatory	Makes the presence of the Service-Type attribute mandatory in RADIUS Access-Accept messages.
on-for-login-auth	Sends the Service-Type attribute in the authentication packets. Note The Service-Type attribute is sent by default in RADIUS Accept-Request messages. Therefore, RADIUS tunnel profiles should include “Service-Type=Outbound” as a check item, not just as a reply item. Failure to include Service-Type=Outbound as a check item can result in a security hole.
support-multiple	Supports multiple Service-Type values for each RADIUS profile.
voice <i>value</i>	Selects the Service-Type value for voice calls. The only value that can be entered is 1. The default is 12.

Command Default

If this command is not configured, the absence of the Service-Type attribute is ignored, and the authentication or authorization does not fail. The default for the **voice** keyword is 12.

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.2(13)T	The mandatory keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If this command is configured and the Service-Type attribute is absent in the Access-Accept message packets, the authentication or authorization fails.

The **support-multiple** keyword allows for multiple instances of the Service-Type attribute to be present in an Access-Accept packet. The default behavior is to disallow multiple instances, which results in an Access-Accept packet containing multiple instances being treated as though an Access-Reject was received.

Examples

The following example shows that the presence of the Service-Type attribute is mandatory in RADIUS Access-Accept messages:

```
Router(config)# radius-server attribute 6 mandatory
```

The following example shows that attribute 6 is to be sent in authentication packets:

```
Router(config)# radius-server attribute 6 on-for-login-auth
```

The following example shows that multiple Service-Type values are to be supported for each RADIUS profile:

```
Router(config)# radius-server attribute 6 support-multiple
```

The following example shows that Service-Type values are to be sent in voice calls:

```
Router(config)# radius-server attribute 6 voice 1
```

radius-server attribute 61 extended

To enable extended, non-RFC-compliant NAS-Port-Type attribute (RADIUS attribute 61), use the **radius-server attribute 61 extended** command in global configuration mode. To disable extended, non-RFC-compliant NAS-Port-Type attribute (RADIUS attribute 61), use the **no** form of this command.

radius-server attribute 61 extended

no radius-server attribute 61 extended

Syntax Description

This command has no arguments or keywords.

Defaults

Extended attribute 61 is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)XI1	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

RADIUS Attribute 61 (Network-attached storage (NAS) port-type, a number) is sent in an access-request to indicate the type of physical port of the NAS, which is authenticating the user with number.

Table 63 NAS Access Technology Values

RADIUS Value	Service Port Type
27	Wireless - IEEE 802.16
30	PPP over ATM (PPPoA)
31	PPP over Ethernet over ATM (PPPoEoA)
32	PPP over Ethernet over Ethernet (PPPoEoE)
33	PPP over Ethernet over VLAN (PPPoEoVLAN)
34	Point-to-Point Protocol over Ethernet IEEE 802.1Q Tunneling (PPPoEoQinQ)

The Value “Virtual” refers to a connection to the NAS through a transport protocol, instead of through a physical port. For example, if a user telnetted into a NAS, the value “Virtual” would be reflected as the NAS value.

There is no specific NAS value for IP sessions. The NAS value depends on the underlying transport technology values described in [Table 63](#) or “Virtual” is used for IP sessions. For example, if PPP is the underlying access technology (transport protocol), the value reported is 33.

If extended attribute 61 is not enabled the following occurs:

radius-server attribute 69 clear

To receive nonencrypted tunnel passwords in attribute 69 (Tunnel-Password), use the **radius-server attribute 69 clear** command in global configuration mode. 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

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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 77

To send connection speed information to the RADIUS server in the access request, use the **radius-server attribute 77** command in global configuration mode. To prevent connection speed information from being included in the access request, use the **no** form of this command.

```
radius-server attribute 77 {include-in-access-req | include-in-acct-req}
```

```
no radius-server attribute 77 {include-in-access-req | include-in-acct-req}
```

Syntax Description

include-in-access-req	Specifies that attribute 77 will be included in access requests.
include-in-acct-req	Specifies that attribute 77 will be included in accounting requests.

Defaults

RADIUS attribute 77 is sent to the RADIUS server in the access request.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)BX	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

RADIUS attribute 77 is sent to the RADIUS server in the access request by default.

RADIUS attribute 77 allows RADIUS authentication based on connection speed. Sessions can be accepted or denied based on the allowed connection speed configured for a particular user on the RADIUS server.

RADIUS attribute 77 includes the following information:

- The accounting start/stop request
- The VC class name defined with the **class-int** command
- The VC class name defined with the **class-vc** command
- The VC class name defined with the **class-range** command

The VC class name may include letters, numbers, and the characters “:” (colon), “;” (semicolon), “-” (hyphen) and “,” (comma).

Examples

The following example disables the inclusion of RADIUS attribute 77 in the access request:

```
no radius-server attribute 77 include-in-access-req
```

Related Commands

Command	Description
class-int	Assigns a VC class to an ATM main interface or subinterface.
class-range	Assigns a VC class to an ATM PVC range.
class-vc	Assigns a VC class to an ATM PVC, SVC, or VC bundle member.

radius-server attribute 8 include-in-access-req

To send the IP address of a user to the RADIUS server in the access request, use the **radius-server attribute 8 include-in-access-req** command in global configuration mode. To disable sending of the user IP address to the RADIUS server during authentication, use the **no** form of this command.

radius-server attribute 8 include-in-access-req

no radius-server attribute 8 include-in-access-req

Syntax Description This command has no arguments or keywords.

Defaults This feature is disabled.

Command Modes Global configuration

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Using the **radius-server attribute 8 include-in-access-req** command makes it possible for a network access server (NAS) to provide the RADIUS server with a hint of the user IP address in advance of user authentication. An application can be run on the RADIUS server to use this hint and build a table (map) of user names and addresses. Using the mapping information, service applications can begin preparing user login information to have available upon successful user authentication.

When a network device dials in to a NAS that is configured for RADIUS authentication, the NAS begins the process of contacting the RADIUS server in preparation for user authentication. Typically, the IP address of the dial-in host is not communicated to the RADIUS server until after successful user authentication. Communicating the device IP address to the server in the RADIUS access request allows other applications to begin to take advantage of that information.

As the NAS is setting up communication with the RADIUS server, the NAS assigns an IP address to the dial-in host from a pool of IP addresses configured at the specific interface. The NAS sends the IP address of the dial-in host to the RADIUS server as attribute 8. At that time, the NAS sends other user information, such as the username, to the RADIUS server.

After the RADIUS server receives the user information from the NAS, it has two options:

- If the user profile on the RADIUS server already includes attribute 8, the RADIUS server can override the IP address sent by the NAS with the IP address defined as attribute 8 in the user profile. The address defined in the user profile is returned to the NAS.

- If the user profile does not include attribute 8, the RADIUS server can accept attribute 8 from the NAS, and the same address is returned to the NAS.

The address returned by the RADIUS server is saved in memory on the NAS for the life of the session. If the NAS is configured for RADIUS accounting, the accounting start packet sent to the RADIUS server includes the same IP address as in attribute 8. All subsequent accounting packets, updates (if configured), and “stop” packets will also include the same IP address as in attribute 8.

**Note**

Configuring the NAS to send the host IP address in the RADIUS access request assumes that the login host is configured to request an IP address from the NAS server. It also assumes that the login host is configured to accept an IP address from the NAS. In addition, the NAS must be configured with a pool of network addresses at the interface supporting the login hosts.

Examples

The following example shows a NAS configuration that sends the IP address of the dial-in host to the RADIUS server in the RADIUS access request. The NAS is configured for RADIUS authentication, authorization, and accounting (AAA). A pool of IP addresses (asyncl-pool) has been configured and applied at interface Async1.

```
aaa new-model
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
!
ip address-pool local
!
interface Async1
 peer default ip address pool asyncl-pool
!
ip local pool asyncl-pool 209.165.200.225 209.165.200.229
!
radius-server host 172.31.71.146 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute 8 include-in-access-req
radius-server key radhost
```

radius-server attribute 30 original-called-number

To allow network providers to accurately match the billing function with the actual number dialed (Original Called Number (OCN)), and not the translated number to which the switch reports, use the **radius-server attribute 30 original-called-number** command in global configuration mode.

radius-server attribute 30 original-called-number

no radius-server attribute 30 original-called-number

Command Default

The command-level default is not enabled. The translated number is sent to the NAS.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3	This command was introduced.

Usage Guidelines

The ITU-T Q.931 attribute is the connection control protocol of the ISDN. Some switches can send a translated dialed number identification service (DNIS) number to the network access server (NAS) instead of the OCN. These switches eventually inform the NAS about the OCN in its Q931 attribute. However, some network providers require the OCN in its Q.931 attribute.

The **radius-server attribute 30 original-called-number** command allows the OCN with its Q.931 attribute to be sent to the RADIUS Called-Station-ID, which is a check mechanism administrators use to deny or accept access from users based on the NAS (when available). This OCN is used instead of the redirected translated number reported as the DNIS by ISDN.

Examples

The following example enables the **radius-server attribute 30 original-called-number** in global configuration mode:

```
aaa new-model
radius-server attribute 30 original-called-number
```

radius-server attribute data-rate send 0



Note

Effective with Cisco IOS Release 12.4, the **radius-server attribute data-rate send 0** command is not available in Cisco IOS software.

To enable the data transmit and receive rate of RADIUS server attributes 197 and 255 in accounting records, use the **radius-server attribute data-rate send 0** command in global configuration mode.

radius-server attribute data-rate send 0

no radius-server attribute data-rate send 0

Syntax Description

This command has no arguments or keywords.

Command Default

The default value for RADIUS server attributes 197 and 255 is zero.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3	This command was introduced.
12.4	This command was removed.

Usage Guidelines

RADIUS attribute 197 is the Ascend-Data-Rate in an accounting-request packet. This attribute specifies the receive baud rate of the connection in bits per second over the course of the connection's lifetime.

RADIUS attribute 255 is the Ascend-Xmit-Rate in an accounting-request packet. This attribute specifies the transmit baud rate of the connection in bits per second over the course of the connection's lifetime.

The connection is authenticated for both RADIUS attributes 197 and 255 if the following conditions are met:

- The session has ended or has failed to authenticate because the accounting-request packet has the RADIUS attribute: Acct-Status-Type=Stop.
- The Auth parameter is set to a value other than RADIUS or LOGOUT.



Note

RADIUS attribute 197 does not appear in the user profile.

Examples

The following example enables the **radius-server attribute data-rate send 0** command in global configuration mode:

```
aaa new-model
radius-server attribute data-rate send 0
```

radius-server attribute list

To define an accept or reject list name, use the **radius-server attribute list** command in global configuration mode. To remove an accept or reject list name from your configuration, use the no form of this command.

radius-server attribute list *list-name*

no radius-server attribute list *list-name*

Syntax Description

list-name Name for an accept or reject list.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.2(1)DX	This command was introduced.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(13)T	Platform support was added for the Cisco 7401 ASR.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

A user may configure an accept or reject list with a selection of attributes on the network access server (NAS) for authorization or accounting so unwanted attributes are not accepted and processed. The **radius-server attribute list** command allows users to specify a name for an accept or reject list. This command is used in conjunction with the **attribute** (server-group configuration) command, which adds attributes to an accept or reject list.



Note

The listname must be the same as the listname defined in the **accounting** or **authorization** configuration command.

Examples

The following example shows how to configure the reject list “bad-author” for RADIUS authorization and accept list “usage-only” for RADIUS accounting:

```
Router(config)# aaa new-model
```

```

Router(config)# aaa authentication ppp default group radius-sg
Router(config)# aaa authorization network default group radius-sg
Router(config)# aaa group server radius radius-sg
Router(config-sg-radius)# server 10.1.1.1
Router(config-sg-radius)# authorization reject bad-author
Router(config-sg-radius)# accounting accept usage-only
Router(config-sg-radius)# exit
Router(config)# radius-server host 10.1.1.1 key mykey1
Router(config)# radius-server attribute list usage-only
Router(config-radius-attrl)# attribute 1,40,42-43,46
Router(config-radius-attrl)# exit
Router(config)# radius-server attribute list bad-author
Router(config-radius-attrl)# attribute 22,27-28,56-59

```

**Note**

Although you cannot configure more than one access or reject list per server group for authorization or accounting, you can configure one list for authorization and one list for accounting per server group.

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
accounting (server-group configuration)	Specifies an accept or reject list for attributes that are to be sent to the RADIUS server in an accounting request.
attribute (server-group configuration)	Adds attributes to an accept or reject list.
authorization (server-group configuration)	Specifies an accept or reject list for attributes that are returned in an Access-Accept packet from the RADIUS server.
radius-server host	Specifies a RADIUS server host.

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 for more information.

radius-server attribute nas-port format

To set the NAS-Port format used for RADIUS accounting features and restore the default NAS-port format, or to set the global attribute 61 session format e string or configure a specific service port type for attribute 61 support, use the **radius-server attribute nas-port format** command in global configuration mode. To stop sending attribute 61 to the RADIUS server, use the **no** form of this command.

NAS-Port for RADIUS Accounting Features and Restoring Default NAS-Port Format

radius-server attribute nas-port format *format*

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

Extended NAS-Port Support

radius-server attribute nas-port format *format* [*string*] [**type** *nas-port-type*]

no radius-server attribute nas-port format *format* [*string*] [**type** *nas-port-type*]

Syntax Description		
<i>format</i>		NAS-Port format. Possible values for the format argument are as follows: <ul style="list-style-type: none"> a—Standard NAS-Port format b—Extended NAS-Port format c—Carrier-based format d—PPPoX (PPP over Ethernet or PPP over ATM) extended NAS-Port format e—Configurable NAS-Port format
<i>string</i>		(Optional) Represents all of a specific port type for format e. It is possible to specify multiple values with this argument.
type <i>nas-port-type</i>		(Optional) Allows you to globally specify different format strings to represent specific physical port types. You may set one of the extended NAS-Port-Type attribute values: <ul style="list-style-type: none"> type 30—PPP over ATM (PPPoA) type 31—PPP over Ethernet (PPPoE) over ATM (PPPoEoA) type 32—PPPoE over Ethernet (PPPoEoE) type 33—PPPoE over VLAN (PPPoEoVLAN) type 34—PPPoE over Q-in-Q (PPPoEoQinQ)

Defaults

Standard NAS-Port format for NAS-Port for RADIUS accounting features and restoring default NAS-Port format or extended NAS-Port support.

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.
12.2(4)T	Format e was introduced.
12.2(11)T	Format e was extended to support PPPoX information.
12.3(3)	Format e was extended to support Session ID U.
12.3(7)XI1	Format e was extended to allow the format string to be NAS-Port-Type attribute specific. The following keyword and arguments were added: <i>string</i> , type <i>nas-port-type</i> .
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

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, virtual path identifier (VPI), and virtual channel indicator (VCI) for PPPoA and PPPoEoA, and the interface and VLAN ID for PPPoE over Institute of Electrical and Electronic Engineers (IEEE) standard 802.1Q VLANs.

Format e

Before Cisco IOS Release 12.2(4)T formats a through c did not work with Cisco platforms such as the AS5400. For this reason, a configurable format e was developed. Format e requires you to explicitly define the usage of the 32 bits of attribute 25 (NAS-Port). The usage is defined with a given parser character for each NAS-Port field of interest for a given bit field. By configuring a single character in a

row, such as x, only one bit is assigned to store that given value. Additional characters of the same type, such as xx, will provide a larger available range of values to be stored. [Table 64](#) shows how the ranges may be expanded:

Table 64 *Format e Ranges*

Character	Range
x	0–1
xx	0–3
xxx	0–7
xxxx	0–F
xxxxx	0–1F

It is imperative that you know what the valid range is for a given parameter on a platform that you want to support. The Cisco IOS RADIUS client will bitmask the determined value to the maximum permissible value on the basis of configuration. Therefore, if one has a parameter that turns out to have a value of 8, but only 3 bits (xxx) are configured, 8 and 0x7 will give a result of 0. Therefore, you must always configure a sufficient number of bits to capture the value required correctly. Care must be taken to ensure that format e is configured to properly work for all NAS port types within your network environment.

[Table 65](#) shows the supported parameters and their characters:

Table 65 *Supported Parameters and Characters*

Supported Parameters	Characters
Zero	0 (always sets a 0 to that bit)
One	1 (always sets a 0 to that bit)
DS0 shelf	f
DS0 slot	s
DS0 adaptor	a
DS0 port	p (physical port)
DS0 subinterface	i
DS0 channel	c
Async shelf	F
Async slot	S
Async port	P
Async line	L (modern line number, that is, physical terminal [TTY] number)
PPPoX slot	S
PPPoX adaptor	A
PPPoX port	P
PPPoX VLAN ID	V
PPPoX VPI	I

Related Commands

Command	Description
radius attribute nas-port-type	Configures subinterfaces such as Ethernet, vLANs, stacked VLAN (Q-in-Q), virtual circuit (VC), and VC ranges.
radius-server attribute 61 extended	Enables extended, non-RFC-compliant NAS-Port-Type attribute (RADIUS attribute 61).
vpdn aaa attribute	Enables the LNS to send PPP extended NAS-Port format values to the RADIUS server for accounting.

radius-server authorization missing Service-Type

The **radius-server authorization missing Service-Type** command is replaced by the **radius-server attribute 6** command. See the **radius-server attribute 6** command for more information.

radius-server backoff exponential

To configure the router for exponential backoff retransmit of accounting requests, use the **radius-server backoff exponential** command in global configuration mode. To disable this functionality, use the **no** form of this command.

radius-server backoff exponential [*max-delay minutes*] [*backoff-retry retransmits*]

no radius-server backoff exponential [*max-delay minutes*] [*backoff-retry retransmits*]

Syntax Description

max-delay <i>minutes</i>	(Optional) Number of retransmissions done in exponential max-delay mode. Valid range for the <i>minutes</i> argument is 1 through 120; if this option is not specified, the default value (60 minutes) will be used.
backoff-retry <i>retransmits</i>	(Optional) Number of retransmissions done in exponential backoff mode in addition to normal and max-delay retransmissions. Valid range for the <i>retransmits</i> argument is 1 through 50; if this option is not specified, the default value (5 retransmits) will be used.

Command Default

This command is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)B	This command was introduced on the Cisco 6400-NRP-1, Cisco 7200 series, and Cisco 7400 series.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The **radius-server backoff exponential** command is used to keep accounting records on a router for up to 24 hours. After enabling this command, the router will try to send the normal retransmissions for the number of times the *retransmits* argument is configured. Thereafter, the router will continue to retransmit accounting requests with an interval that doubles on each retransmit failure until a configured maximum interval is reached.

While the router is in “retransmit mode,” it will store all accounting records that are generated during that period in its memory; the accounting records will be sent to the RADIUS server after the router comes back up before the retransmit mode is complete.

Examples

The following example shows how to configure your router for exponential backoff retransmit of accounting requests:

```
aaa new-model
aaa authentication login default group radius
aaa authentication ppp default group radius
aaa authorization exec default group radius
```

■ radius-server backoff exponential

```

aaa authorization network default group radius
aaa accounting send stop-record authentication failure
aaa accounting update periodic 1
aaa accounting network default start-stop group radius
!
interface BRI1/0
 ip address 10.0.0.2 255.0.0.0
 encapsulation ppp
 no ip mroute-cache
 dialer idle-timeout 0
 dialer-group 1
 isdn switch-type basic-5ess
!
radius-server host 172.107.164.206 auth-port 1645 acct-port 1646 backoff exponential
max-delay 60 backoff-retry 32
radius-server backoff exponential max-delay 60 backoff-retry 32
radius-server retransmit 3
radius-server key rad123
end

```

Related Commands

Command	Description
backoff exponential	Configures the router for exponential backoff retransmit of accounting requests per RADIUS server group.
radius-server host	Specifies a RADIUS server host.

radius-server challenge-noecho

To prevent user responses to Access-Challenge packets from being displayed on the screen, use the **radius-server challenge-noecho** command in global configuration mode. 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.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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*.

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.
	12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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 dead-criteria

To force one or both of the criteria—used to mark a RADIUS server as dead—to be the indicated constant, use the **radius-server dead-criteria** command in global configuration mode. To disable the criteria that were set, use the **no** form of this command.

radius-server dead-criteria [**time** *seconds*] [**tries** *number-of-tries*]

no radius-server dead-criteria [**time** *seconds* | **tries** *number-of-tries*]

Syntax Description

time <i>seconds</i>	<p>(Optional) Minimum amount of time, in seconds, that must elapse from the time that the router last received a valid packet from the RADIUS server to the time the server is marked as dead. If a packet has not been received since the router booted, and there is a timeout, the time criterion will be treated as though it has been met. You can configure the time to be from 1 through 120 seconds.</p> <ul style="list-style-type: none"> If the <i>seconds</i> argument is not configured, the number of seconds will range from 10 to 60 seconds, depending on the transaction rate of the server. <p>Note Both the time criterion and the tries criterion must be met for the server to be marked as dead.</p>
tries <i>number-of-tries</i>	<p>(Optional) Number of consecutive timeouts that must occur on the router before the RADIUS server is marked as dead. If the server performs both authentication and accounting, both types of packets will be included in the number. Improperly constructed packets will be counted as though they were timeouts. All transmissions, including the initial transmit and all retransmits, will be counted. You can configure the number of timeouts to be from 1 through 100.</p> <ul style="list-style-type: none"> If the <i>number-of-tries</i> argument is not configured, the number of consecutive timeouts will range from 10 to 100, depending on the transaction rate of the server and the number of configured retransmissions. <p>Note Both the time criterion and the tries criterion must be met for the server to be marked as dead.</p>

Command Default

The number of seconds and number of consecutive timeouts that occur before the RADIUS server is marked as dead will vary, depending on the transaction rate of the server and the number of configured retransmissions.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.

Release	Modification
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines



Note

Both the time criterion and the tries criterion must be met for the server to be marked as dead.

The **no** form of this command has the following cases:

- If neither the *seconds* nor the *number-of-tries* argument is specified with the **no radius-server dead-criteria** command, both time and tries will be reset to their defaults.
- If the *seconds* argument is specified using the originally set value, the time will be reset to the default value range (10 to 60).
- If the *number-of-tries* argument is specified using the originally set value, the number of tries will be reset to the default value range (10 to 100).

Examples

The following example shows how to configure the router so that it will be considered dead after 5 seconds and 4 tries:

```
Router (config)# radius-server dead-criteria time 5 tries 4
```

The following example shows how to disable the time and number-of-tries criteria that were set for the **radius-server dead-criteria** command.

```
Router (config)# no radius-server dead-criteria
```

The following example shows how to disable the time criterion that was set for the **radius-server dead-criteria** command.

```
Router (config)# no radius-server dead-criteria time 5
```

The following example shows how to disable the number-of-tries criterion that was set for the **radius-server dead-criteria** command.

```
Router (config)# no radius-server dead-criteria tries 4
```

Related Commands

Command	Description
debug aaa dead-criteria transactions	Displays AAA dead-criteria transaction values.
show aaa dead-criteria	Displays dead-criteria information for a AAA server.
show aaa server-private	Displays the status of all private RADIUS servers.
show aaa servers	Displays information about the number of packets sent to and received from AAA servers.

radius-server deadline

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

radius-server deadline *minutes*

no radius-server deadline

Syntax Description

<i>minutes</i>	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.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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.”

When the RADIUS Server Is Marked As Dead

For Cisco IOS versions prior to 12.2(13.7)T, the RADIUS server will be marked as dead if a transaction is transmitted for the configured number of retransmits and a valid response is not received from the server within the configured timeout for any of the RADIUS packet transmissions.

For Cisco IOS versions 12.2(13.7)T and later, the RADIUS server will be marked as dead if both of the following conditions are met:

1. A valid response has not been received from the RADIUS server for any outstanding transaction for at least the timeout period that is used to determine whether to retransmit to that server, and
2. Across all transactions being sent to the RADIUS server, at least the requisite number of retransmits +1 (for the initial transmission) have been sent consecutively without receiving a valid response from the server with the requisite timeout.

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 network 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.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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.



Note

If a private RADIUS server is used as the group server by configuring the **server-private** (RADIUS) command, then the **radius-server directed-request** command cannot be configured.

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
```

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.
server-private (RADIUS)	Configures the IP address of the private RADIUS server for the group server.

radius-server domain-stripping

To configure a network access server (NAS) to strip suffixes, or to strip both suffixes and prefixes from the username before forwarding the username to the remote RADIUS server, use the **radius-server domain-stripping** command in global configuration mode. To disable a stripping configuration, use the **no** form of this command.

radius-server domain-stripping [[**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] | **strip-suffix** *suffix*] [**vrf** *vrf-name*]

no radius-server domain-stripping [[**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] | **strip-suffix** *suffix*] [**vrf** *vrf-name*]

Syntax Description

right-to-left	(Optional) Specifies that the NAS will apply the stripping configuration at the first delimiter found when parsing the full username from right to left. The default is for the NAS to apply the stripping configuration at the first delimiter found when parsing the full username from left to right.
prefix-delimiter <i>character</i> [<i>character2...character7</i>]	(Optional) Enables prefix stripping and specifies the character or characters that will be recognized as a prefix delimiter. Valid values for the <i>character</i> argument are @, /, \$, %, \, #, and -. Multiple characters can be entered without intervening spaces. Up to seven characters can be defined as prefix delimiters, which is the maximum number of valid characters. If a \ is entered as the final or only value for the <i>character</i> argument, it must be entered as \\. No prefix delimiter is defined by default.
delimiter <i>character</i> [<i>character2...character7</i>]	(Optional) Specifies the character or characters that will be recognized as a suffix delimiter. Valid values for the <i>character</i> argument are @, /, \$, %, \, #, and -. Multiple characters can be entered without intervening spaces. Up to seven characters can be defined as suffix delimiters, which is the maximum number of valid characters. If a \ is entered as the final or only value for the <i>character</i> argument, it must be entered as \\. The default suffix delimiter is the @ character.
strip-suffix <i>suffix</i>	(Optional) Specifies a suffix to strip from the username.
vrf <i>vrf-name</i>	(Optional) Restricts the domain stripping configuration to a Virtual Private Network (VPN) routing and forwarding (VRF) instance. The <i>vrf-name</i> argument specifies the name of a VRF.

Command Default

Stripping is disabled. The full username is sent to the RADIUS server.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)DD	This command was introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(4)T	Support was added for the right-to-left and delimiter <i>character</i> keywords and argument.
12.4(4)T	Support was added for the strip-suffix <i>suffix</i> and prefix-delimiter keywords and argument.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.(33)SRC.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **radius-server domain-stripping** command to configure the NAS to strip the domain from a username before forwarding the username to the RADIUS server. If the full username is `user1@cisco.com`, enabling the **radius-server domain-stripping** command results in the username “user1” being forwarded to the RADIUS server.

Use the **right-to-left** keyword to specify that the username should be parsed for a delimiter from right to left, rather than from left to right. This allows strings with two instances of a delimiter to strip the username at either delimiter. For example, if the username is `user@cisco.com@cisco.net`, the suffix could be stripped in two ways. The default direction (left to right) would result in the username “user” being forwarded to the RADIUS server. Configuring the **right-to-left** keyword would result in the username “user@cisco.com” being forwarded to the RADIUS server.

Use the **prefix-delimiter** keyword to enable prefix stripping and to specify the character or characters that will be recognized as a prefix delimiter. The first configured character that is parsed will be used as the prefix delimiter, and any characters before that delimiter will be stripped.

Use the **delimiter** keyword to specify the character or characters that will be recognized as a suffix delimiter. The first configured character that is parsed will be used as the suffix delimiter, and any characters after that delimiter will be stripped.

Use **strip-suffix** *suffix* to specify a particular suffix to strip from usernames. For example, configuring the **radius-server domain-stripping strip-suffix cisco.net** command would result in the username `user@cisco.net` being stripped, while the username `user@cisco.com` will not be stripped. You may configure multiple suffixes for stripping by issuing multiple instances of the **radius-server domain-stripping** command. The default suffix delimiter is the `@` character.



Note

Issuing the **radius-server domain-stripping strip-suffix** *suffix* command disables the capacity to strip suffixes from all domains. Both the suffix delimiter and the suffix must match for the suffix to be stripped from the full username. The default suffix delimiter of `@` will be used if you do not specify a different suffix delimiter or set of suffix delimiters using the **delimiter** keyword.

To apply a domain-stripping configuration only to a specified VRF, use the **vrf** *vrf-name* option.

The interactions between the different types of domain stripping configurations are as follows:

- You may configure only one instance of the **radius-server domain-stripping** [right-to-left] [prefix-delimiter *character* [*character2...character7*]] [delimiter *character* [*character2...character7*]] command.
- You may configure multiple instances of the **radius-server domain-stripping** [right-to-left] [prefix-delimiter *character* [*character2...character7*]] [delimiter *character* [*character2...character7*]] [vrf *vrf-name*] command with unique values for vrf *vrf-name*.
- You may configure multiple instances of the **radius-server domain-stripping strip-suffix** *suffix* [vrf *per-vrf*] command to specify multiple suffixes to be stripped as part of a global or per-VRF ruleset.
- Issuing any version of the **radius-server domain-stripping** command automatically enables suffix stripping using the default delimiter character @ for that ruleset, unless a different delimiter or set of delimiters is specified.
- Configuring a per-suffix stripping rule disables generic suffix stripping for that ruleset. Only suffixes that match the configured suffix or suffixes will be stripped from usernames.

Examples

The following example configures the router to parse the username from right to left and sets the valid suffix delimiter characters as @, \, and \$. If the full username is cisco/user@cisco.com\$cisco.net, the username “cisco/user@cisco.com” will be forwarded to the RADIUS server because the \$ character is the first valid delimiter encountered by the NAS when parsing the username from right to left.

```
radius-server domain-stripping right-to-left delimiter @\%
```

The following example configures the router to strip the domain name from usernames only for users associated with the VRF instance named abc. The default suffix delimiter @ will be used for generic suffix stripping.

```
radius-server domain-stripping vrf abc
```

The following example enables prefix stripping using the character / as the prefix delimiter. The default suffix delimiter character @ will be used for generic suffix stripping. If the full username is cisco/user@cisco.com, the username “user” will be forwarded to the RADIUS server.

```
radius-server domain-stripping prefix-delimiter /
```

The following example enables prefix stripping, specifies the character / as the prefix delimiter, and specifies the character # as the suffix delimiter. If the full username is cisco/user@cisco.com#cisco.net, the username “user@cisco.com” will be forwarded to the RADIUS server.

```
radius-server domain-stripping prefix-delimiter / delimiter #
```

The following example enables prefix stripping, configures the character / as the prefix delimiter, configures the characters \$, @, and # as suffix delimiters, and configures per-suffix stripping of the suffix cisco.com. If the full username is cisco/user@cisco.com, the username “user” will be forwarded to the RADIUS server. If the full username is cisco/user@cisco.com#cisco.com, the username “user@cisco.com” will be forwarded.

```
radius-server domain-stripping prefix-delimiter / delimiter $@#
radius-server domain-stripping strip-suffix cisco.com
```

The following example configures the router to parse the username from right to left and enables suffix stripping for usernames with the suffix cisco.com. If the full username is cisco/user@cisco.net@cisco.com, the username “cisco/user@cisco.net” will be forwarded to the RADIUS server. If the full username is cisco/user@cisco.com@cisco.net, the full username will be forwarded.

```
radius-server domain-stripping right-to-left
radius-server domain-stripping strip-suffix cisco.com
```

The following example configures a set of global stripping rules that will strip the suffix `cisco.com` using the delimiter `@`, and a different set of stripping rules for usernames associated with the VRF named `myvrf`:

```
radius-server domain-stripping strip-suffix cisco.com
!
radius-server domain-stripping prefix-delimiter # vrf myvrf
radius-server domain-stripping strip-suffix cisco.net vrf myvrf
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
ip vrf	Defines a VRF instance and enters VRF configuration mode.
tacacs-server domain-stripping	Configures a router to strip a prefix or suffix from the username before forwarding the username to the TACACS+ server.

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 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.

Cisco IOS Releases 12.2SB and 12.2SR

```
radius-server host {hostname | ip-address} [test username user-name] [auth-port port-number]
[ignore-auth-port] [acct-port port-number] [ignore-acct-port] [timeout seconds]
[retransmit retries] [key string] [alias {hostname | ip-address}] [idle-time minutes] [backoff
exponential {backoff-retry number-of-retransmits | max-delay minutes}] [key
encryption-key]
```

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

All Other Releases

```
radius-server host {hostname | ip-address} [auth-port port-number] [acct-port port-number]
[timeout seconds] [retransmit retries] [key string] [alias {hostname | ip-address}] [backoff
exponential {backoff-retry number-of-retransmits | max-delay minutes}] [pac [key
encryption-key] | key encryption-key]
```

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

Syntax Description		
<i>hostname</i>		Domain Name System (DNS) name of the RADIUS server host.
<i>ip-address</i>		IP address of the RADIUS server host.
test username		(Optional) Turns on the automated testing feature for RADIUS server load balancing.
<i>user-name</i>		(Optional) Test user ID username.
auth-port		(Optional) Specifies the User Datagram Protocol (UDP) destination port for authentication requests.
<i>port-number</i>		(Optional) The port number for authentication requests; the host is not used for authentication if the port number is set to 0. If the port number is not specified, the port number defaults to 1645.
ignore-auth-port		(Optional) Turns off the automated testing feature for RADIUS server load balancing on the authentication port.
acct-port		(Optional) Specifies the UDP destination port for accounting requests.
ignore-acct-port		(Optional) Turns off the automated testing feature for RADIUS server load balancing on the accounting port.
timeout <i>seconds</i>		(Optional) Specifies 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.
retransmit <i>retries</i>		(Optional) Specifies the number of times a RADIUS request is re-sent to a server, if that server is not responding or is responding slowly. This setting overrides the global setting of the radius-server retransmit command. If no retransmit value is specified, the global value is used. Enter a value in the range 1 to 100.

key	(Optional) Specifies the authentication and encryption key used between the router and the RADIUS daemon running on this RADIUS server. This key overrides the global setting of the radius-server key command. If no key string is specified, the global value is used. The key is a text string that must match the encryption key used on the RADIUS server. Always configure the key as the last item in the radius-server host command syntax. This is because the leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.
<i>string</i>	(Optional) 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.
idle-time <i>minutes</i>	(Optional) Specifies the length of time the server remains idle before it is quarantined and test packets are sent out. <ul style="list-style-type: none"> • Default is 60 minutes (1 hour). • The valid range is 1 to 35791 seconds.
backoff exponential	(Optional) Specifies the exponential retransmits backup mode.
backoff-retry <i>number-of-retransmits</i>	Specifies the exponential backoff retry. <ul style="list-style-type: none"> • <i>number-of-retransmits</i>—Number of backoff retries. Value = 1 through 50. The default is 8.
max-delay <i>minutes</i>	Specifies the maximum delay between retransmits. <ul style="list-style-type: none"> • <i>minutes</i>—Value = 1 through 120 minutes. The default is 3 minutes.
pac	(Optional) Specifies that automatic Protected Access Credential (PAC) provisioning is triggered. Note The pac keyword is mutually exclusive with the shared secret key keyword that already exists.
key <i>encryption-key</i>	Specifies the per-server encryption key (overrides the default). <ul style="list-style-type: none"> • <i>encryption-key</i>—Can be 0 (specifies that an unencrypted keys follows), 7 (specifies that a hidden key follows), or a line specifying the unencrypted (clear-text) server key.

Defaults

No RADIUS host is specified; use global **radius-server** command values.
RADIUS server load balancing automated testing is disabled by default.

Command Modes

Global configuration (config)

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.
12.2(15)B	The backoff exponential , backoff-retry , key , and max-delay keywords and <i>number-of-retransmits</i> , <i>encryption-key</i> , and <i>minutes</i> arguments were added.
12.2(28)SB	The test username <i>user-name</i> , ignore-auth-port , ignore-acct-port , and idle-time <i>seconds</i> keywords and arguments were added for configuring RADIUS server load balancing automated testing functionality. Note The keywords and arguments added in Cisco IOS Release 12.2(28)SB apply to any subsequent 12.2SB releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. The keywords and arguments that were added in Cisco IOS Release 12.2(28)SB apply to Cisco IOS Release 12.2(33)SRA and subsequent 12.2SR releases.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T. Note The keywords and arguments that were added in Cisco IOS Release 12.2(28)SB do not apply to Cisco IOS Release 12.4(11)T or to subsequent 12.4T releases.
12.2 SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. Note The keywords and arguments that were added in Cisco IOS Release 12.2(28)SB do not apply to Cisco IOS Release 12.2SX.

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.

You can specify the keywords of the **radius-server host** command in any order. However, the **pac** keyword always precedes the **key** *encryption-key* keyword.

If you do not specify the port number for authentication requests for both the **acct-port** and the **auth-port** keywords, the port number defaults to 1645.

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

We recommend the use of a test user who is not defined on the RADIUS server for the automated testing of the RADIUS server. This is to protect against security issues that can arise if the test user is not configured correctly.

If you configure one RADIUS server with the nonstandard option and another RADIUS server without the nonstandard option, the RADIUS-server host with the nonstandard option does not accept a predefined host. If you configure the same RADIUS server host IP address for a different UDP destination port for accounting requests using the **acct-port** keyword and a UDP destination port for authentication requests using the **auth-port** keyword with and without the nonstandard option, the RADIUS server does not accept the nonstandard option.

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.

RADIUS Server Automated Testing (for Cisco IOS Release 12.2(28)SB)

When you use the **radius-server host** command to enable automated testing for RADIUS server load balancing:

- The authentication port is enabled by default. If the port number is not specified, the default port of 1645 is used. To disable the authentication port, specify the **ignore-auth-port** keyword.
- The accounting port is enabled by default. If the port number is not specified, the default port of 1645 is used. To disable the accounting port, specify the **ignore-acct-port** keyword.

Examples

Releases Other than Cisco IOS Release 12.2(28)SB

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 192.0.2.46 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 192.0.2.46 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 192.0.2.1:

```
radius-server host 192.0.2.1 auth-port 1646 acct-port 1645
radius-server host 192.0.2.1 alias 192.0.2.2 192.0.2.3 192.0.2.4
```

The following example shows how to enable exponential backoff retransmits on a per-server basis. In this example, assume that the retransmit is configured for three retries and the timeout is configured for 5 seconds; that is, the RADIUS request will be transmitted three times with a delay of 5 seconds. Thereafter, the router will continue to retransmit RADIUS requests with a delayed interval that doubles each time until 32 retries have been achieved. The router will stop doubling the retransmit intervals after the interval surpasses the configured 60 minutes; it will transmit every 60 minutes.

The **pac** keyword allows the PAC-Opaque, which is a variable length field, to be sent to the server during the Transport Layer Security (TLS) tunnel establishment phase. The PAC-Opaque can be interpreted only by the server to recover the required information for the server to validate the peer’s identity and authentication. For example, the PAC-Opaque may include the PAC-Key and the PAC’s peer identity. The PAC-Opaque format and contents are specific to the issuing PAC server.

The following example configures automatic PAC provisioning on a router. In seed devices, also known as core switches, the PAC-Opaque has to be provisioned so that all RADIUS exchanges can use this PAC-Opaque to enable automatic PAC provisioning for the server being used. All nonseed devices obtain the PAC-Opaque during the authentication phase of a link initialization.

```
enable
configure terminal
radius-server host 10.0.0.1 auth-port 1812 acct-port 1813 pac
```

Cisco IOS Release 12.2(28)SB

The following example shows how to enable RADIUS server automated testing for load balancing with the authorization and accounting ports specified:

```
radius-server host 192.0.2.176 test username test1 auth-port 1645 acct-port 1646
```

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.
debug aaa test	Shows when the idle timer or dead timer has expired for RADIUS server load balancing.
load-balance	Enables RADIUS server load balancing for named RADIUS server groups.
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 load-balance	Enables RADIUS server load balancing for the global RADIUS server group.
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.
test aaa group	Tests RADIUS load balancing server response manually.
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 {*host-name* | *ip-address*} **non-standard**

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

Syntax Description

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

Defaults

No RADIUS host is specified.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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.
<i>string</i>	The unencrypted (cleartext) shared key.
7	Specifies that a hidden key will follow.
<i>string</i>	The hidden shared key.
<i>string</i>	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 <i>string</i> argument was modified as follows: <ul style="list-style-type: none"> • 0 string • 7 string • <i>string</i>
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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:

```
Router# 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 load-balance

To enable RADIUS server load balancing for the global RADIUS server group referred to as “radius” in the authentication, authorization and accounting (AAA) method lists, use the **radius-server load-balance** command in global configuration mode. To disable RADIUS server load balancing, use the **no** form of this command.

radius-server load-balance method least-outstanding [*batch-size number*]
[*ignore-preferred-server*]

no radius-server load-balance

Syntax Description

method least-outstanding	Enables least outstanding mode for load balancing.
batch-size	(Optional) The number of transactions to be assigned per batch.
<i>number</i>	(Optional) The number of transactions in a batch. <ul style="list-style-type: none"> The default is 25. The range is 1–2147483647. <p>Note Batch size may impact throughput and CPU load. It is recommended that the default batch size, 25, be used because it is optimal for high throughput, without adversely impacting CPU load.</p>
ignore-preferred-server	(Optional) Indicates if a transaction associated with a single AAA session should attempt to use the same server or not. <ul style="list-style-type: none"> If set, preferred server setting will not be used. Default is to use the preferred server.

Command Defaults

If this command is not configured, global RADIUS server load balancing will not occur.

Command Modes

Global configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Examples

The following example shows how to enable load balancing for global RADIUS server groups. It is shown in three parts: the current configuration of RADIUS command output, debug output, and AAA server status information. You can use the delimiting characters to display only the relevant parts of the configuration.

Server Configuration and Enabling Load Balancing for Global RADIUS Server Group Example

The following shows the relevant RADIUS configuration:

```
Router# show running-config | inc radius

aaa authentication ppp default group radius
aaa accounting network default start-stop group radius
radius-server host 192.0.2.238 auth-port 2095 acct-port 2096 key cisco
radius-server host 192.0.2.238 auth-port 2015 acct-port 2016 key cisco
radius-server load-balance method least-outstanding batch-size 5
```

The lines in the current configuration of RADIUS command output above are defined as follows:

- The **aaa authentication ppp** command authenticates all PPP users using RADIUS.
- The **aaa accounting** command enables the sending of all accounting requests to the AAA server after the client is authenticated and after the disconnect using the keyword start-stop.
- The **radius-server host** command defines the IP address of the RADIUS server host with the authorization and accounting ports specified and the authentication and encryption key identified.
- The **radius-server load-balance** command enables load balancing for the global RADIUS server groups with the batch size specified.

Debug Output for Global RADIUS Server Group Example

The debug output below shows the selection of preferred server and processing of requests for the configuration above.

```
Router# show debug

General OS:
  AAA server group server selection debugging is on
Router#
<sending 10 pppoe requests>
Router#
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000014):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[0] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000014):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000015):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000015):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000016):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000016):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000017):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
```

```

*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000017):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000018):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000018):Server (192.0.2.238:2095,2096) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000019):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(00000019):Server (192.0.2.238:2015,2016) now
being used as preferred server
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT(0000001A):No preferred server available.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.199:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT(0000001A):Server (192.0.2.238:2015,2016) now
being used as preferred server
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT(0000001B):No preferred server available.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT(0000001B):Server (192.0.2.238:2015,2016) now
being used as preferred server
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT(0000001C):No preferred server available.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT(0000001C):Server (192.0.2.238:2015,2016) now
being used as preferred server
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT(0000001D):No preferred server available.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:40:32.203:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server
.
.
.

```

Server Status Information for Global RADIUS Server Group Example

The output below shows the AAA server status for the global RADIUS server group configuration example.

```
Router# show aaa server
```

```

RADIUS:id 4, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
State:current UP, duration 3175s, previous duration 0s
Dead:total time 0s, count 0
Quarantined:No
Authen:request 6, timeouts 1
      Response:unexpected 1, server error 0, incorrect 0, time 1841ms
      Transaction:success 5, failure 0
Author:request 0, timeouts 0
      Response:unexpected 0, server error 0, incorrect 0, time 0ms
      Transaction:success 0, failure 0
Account:request 5, timeouts 0
      Response:unexpected 0, server error 0, incorrect 0, time 3303ms
      Transaction:success 5, failure 0

```

```

Elapsed time since counters last cleared:2m

RADIUS:id 5, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
State:current UP, duration 3175s, previous duration 0s
Dead:total time 0s, count 0
Quarantined:No
Authen:request 6, timeouts 1
    Response:unexpected 1, server error 0, incorrect 0, time 1955ms
    Transaction:success 5, failure 0
Author:request 0, timeouts 0
    Response:unexpected 0, server error 0, incorrect 0, time 0ms
    Transaction:success 0, failure 0
Account:request 5, timeouts 0
    Response:unexpected 0, server error 0, incorrect 0, time 3247ms
    Transaction:success 5, failure 0
Elapsed time since counters last cleared:2m
Router#

```

The output shows the status of two RADIUS servers. Both servers are up and, in the last 2 minutes, have processed successfully:

- 5 out of 6 authentication requests
- 5 out of 5 accounting requests

Related Commands

Command	Description
debug aaa sg-server selection	Shows why the RADIUS and TACACS+ server group system in a router is selecting a particular server.
debug aaa test	Shows when the idle timer or dead timer has expired for RADIUS server load balancing.
load-balance	Enables RADIUS server load balancing for named RADIUS server groups.
radius-server host	Enables RADIUS automated testing for load balancing.
test aaa group	Tests RADIUS load balancing server response manually.

radius-server local

To enable the access point or wireless-aware router as a local authentication server and to enter into configuration mode for the authenticator, use the **radius-server local** command in global configuration mode. To remove the local RADIUS server configuration from the router or access point, use the **no** form of this command.

radius-server local

no radius-server local

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values

Command Modes Global configuration

Command History	Release	Modification
	12.2(11)JA	This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.
	12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.
	12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples The following example shows that the access point is being configured to serve as a local authentication server:

```
Router(config)# radius-server local
```

Usage Guidelines This command is not supported on bridges.

Related Commands	Command	Description
	block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
	clear radius local-server	Clears the statistics display or unblocks a user.
	debug radius local-server	Displays the debug information for the local server.

Command	Description
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

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.
	12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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	<i>retries</i> Maximum number of retransmission attempts. The range is 0 to 100. The default is 3.
---------------------------	--

Defaults	3 attempts
-----------------	------------

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

Command History	Release	Modification
	11.1	This command was introduced.
	12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

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

If the RADIUS server is only a few hops from the router, we recommend that you configure the RADIUS server retransmit rate to 5.

Examples	The following example shows how to specify a retransmit counter value of five times:
-----------------	--

```
radius-server retransmit 5
```

Related Commands	Command	Description
	radius-server host	Specifies a RADIUS server host.
	radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
	radius-server timeout	Sets the interval for which a router waits for a server host to reply.
	show radius statistics	Displays the RADIUS statistics for accounting and authentication packets.

radius-server retry method reorder

To specify the reordering of RADIUS traffic retries among a server group, use the **radius-server retry method reorder** command in global configuration mode. To disable the reordering of retries among the server group, use the **no** form of this command.

radius-server retry method reorder

no radius-server retry method reorder

Syntax Description This command has no arguments or keywords.

Defaults If this command is not configured, RADIUS traffic is not reordered among the server group.

Command Modes Global configuration

Command History	Release	Modification
	12.3(1)	This command was introduced.
	12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines Use this command to reorder RADIUS traffic to another server in the server group when the first server fails in periods of high load. Subsequent to the failure, all RADIUS traffic is directed to the new server. Traffic is switched from the new server to another server in the server group only if the new server also fails. Traffic will not be automatically switched back to the first server.

If the **radius-server retry method reorder** command is not configured, each RADIUS server is used until marked dead. The nondead server that is closest to the beginning of the list is used for the first transmission of a transaction and for the configured number of retransmissions. Each nondead server in the list is thereafter tried in turn.

Examples The following example shows that RADIUS server retry has been configured:

```
aaa new-model
radius-server retry method reorder
radius-server retransmit 0
radius-server transaction max-tries 6
radius-server host 192.2.3.4 key rad123
radius-server host 192.5.6.7 key rad123
```

Related Commands

Command	Description
radius-server transaction max-tries	Specifies the maximum number of transmissions that may be retried per transaction on a RADIUS server.

radius-server source-ports extended

To enable 200 ports in the range from 21645 to 21844 to be used as the source ports for sending out RADIUS requests, use the **radius-server source-ports extended** command in global configuration mode. To return to the default setting, in which ports 1645 and 1646 are used as the source ports for RADIUS requests, use the **no** form of this command.

radius-server source-ports extended

no radius-server source-ports extended

Syntax Description This command has no arguments or keywords.

Defaults Ports 1645 and 1646 are used as the source ports for RADIUS requests.

Command Modes Global configuration

Command History	Release	Modification
	12.3(4)	This command was introduced.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines The identifier field of the RADIUS packet is 8 bits long, and yields 256 unique identifiers. A NAS uses one port (1645) as the source port to send out access requests to the RADIUS server and one port (1646) as the source port to send out accounting requests to the RADIUS server. This scheme allows for 256 outstanding access requests and 256 outstanding accounting requests.

If the number of outstanding access requests or accounting requests exceeds 256, the port and ID space will wrap, and all subsequent RADIUS requests will be forced to reuse ports and IDs that are already in use. When the RADIUS server receives a request that uses a port and ID that is already in use, it treats the request as a duplicate. The RADIUS server then drops the request.

The **radius-server source-ports extended** command allows you to configure the NAS to use 200 ports in the range from 21645 to 21844 as the source ports for sending out RADIUS requests. Having 200 source ports allows up to 256*200 authentication and accounting requests to be outstanding at one time. During peak call volume, typically when a router first boots or when an interface flaps, the extra source ports allow sessions to recover more quickly on large-scale aggregation platforms.

Examples The following example shows how to configure a NAS to use 200 ports in the range from 21645 to 21844 as the source ports for RADIUS requests:

```
Router(config)# radius-server source-ports extended
```

radius-server throttle

To configure throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server, use the **radius-server throttle** command in global configuration mode. To disable throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server, use the **no** form of this command.

```
radius-server throttle {[accounting threshold] [access threshold [access-timeout
number-of-timeouts]]}
```

```
no radius-server throttle {[accounting threshold] [access threshold [access-timeout
number-of-timeouts]]}
```

Syntax Description	
accounting threshold	Configures the threshold value for accounting requests sent to a RADIUS server. The range is 0 through 65536. The default value is 0 (throttling disabled).
access threshold	Configures the threshold value for access requests sent to a RADIUS server. The range is 0 through 65536. The default value is 0 (throttling disabled).
access-timeout <i>number-of-timeouts</i>	(Optional) Specifies the number of consecutive access timeouts that are allowed before the access request is dropped. The range is 1 through 10. The default value is 3.

Command Default Throttling is disabled.

Command Modes Global configuration (config)

Command History	Release	Modification
	12.2(33)SRC	This command was introduced.
	12.2(33)SB	This command was implemented on the Cisco 10,000 series routers.
	12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines Use this command to configure throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server.

Examples The following examples show how to configure throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server.

The following example shows how to limit the number of accounting requests sent to a RADIUS server to 100:

```
Router> enable
Router# configure terminal
Router(config)# radius-server throttle accounting 100
```

The following example shows how to limit the number of access request packets sent to a RADIUS server to 200 and sets the number of timeouts allowed per transactions to 2:

```
Router> enable
Router# configure terminal
Router(config)# radius-server throttle access 200
Router(config)# radius-server throttle access 200 access-timeout 2
```

The following example shows how to throttle both accounting and access request packets:

```
Router> enable
Router# configure terminal
Router(config)# radius-server throttle accounting 100 access 200
```

Related Commands

Command	Description
radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server retransmit	Specifies the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
radius-server timeout	Specifies the number of seconds a router waits for a server host to reply before timing out.
show radius statistics	Displays the RADIUS statistics for accounting and authentication packets.
throttle	Configures server group throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server.

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	<i>seconds</i>	Number that specifies the timeout interval, in seconds. The range is 1 to 1000. The default is 5 seconds.
---------------------------	----------------	---

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

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

Command History	Release	Modification
	11.1	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.	
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.	

Usage Guidelines	Use this command to set the number of seconds a router waits for a server host to reply before timing out. If the RADIUS server is only a few hops from the router, we recommend that you configure the RADIUS server timeout to 15 seconds.
-------------------------	--

Examples	The following example shows how to set 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 retransmit	Specifies the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up.	
show radius statistics	Displays the RADIUS statistics for accounting and authentication packets.	

radius-server transaction max-tries

To specify the maximum number of transmissions that may be retried per transaction on a RADIUS server, use the **radius-server transaction max-retries** command in global configuration mode. To disable the number of retries that were configured, use the **no** form of this command.

radius-server transaction max-tries *number*

no radius-server transaction max-tries *number*

Syntax Description

number Total number of transmissions per transaction. The default is eight.

Defaults

Eight transmissions

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Use this command to specify the maximum number of transmissions that may be retried per transaction on a RADIUS server. This command has no meaning if the **radius-server retry method order** command has not been already configured.

Examples

The following example shows that a RADIUS server has been configured for six retries per transaction:

```
aaa new-model
radius-server retry method reorder
radius-server retransmit 0
radius-server transaction max-tries 6
radius-server host 192.2.3.4
radius-server host 192.6.7.8
```

Related Commands

Command	Description
radius-server retry method reorder	Specifies the reordering of RADIUS traffic retries among a server group.

radius-server unique-ident

To enable the `acct-session-id-count` variable containing the unique identifier variable, use the **radius-server unique-ident** command in global configuration mode. To disable the `acct-session-id-count` variable, use the **no** form of this command.

radius-server unique-ident *id*

no radius-server unique-ident

Syntax Description

<i>id</i>	Unique identifier represented by the first eight bits of the <code>acct-session-id-count</code> variable. Valid values range from 0 to 255.
-----------	---

Defaults

The `acct-session-id-count` variable is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.

Usage Guidelines

Use the **radius-server unique-ident** command to increase the size of the accounting session identifier (ID) variable from 32 bits to 56 bits.

RADIUS attribute 44, Accounting Session ID, is a unique accounting identifier that makes it easy to match start and stop records in a log file. Accounting session ID numbers restart at 1 each time the router is power-cycled or the software is reloaded.

The `acct-session-id` variable is a 32-bit variable that can take on values from 00000000–FFFFFFFF.

The `acct-session-id-count` variable enabled by the **radius-server unique-ident** command is a 32-bit variable. The first eight bits of the variable are reserved for the unique identifier, an identifier that allows the RADIUS server to identify an accounting session if a reload occurs. The remaining 24 bits of the `acct-session-id-count` variable acts as a counter variable. When the first `acct-session-id` variable is assigned, the `acct-session-id-count` variable is set to 1. The `acct-session-id-count` variable increments by one every time the `acct-session-id` variable wraps.

The `acct-session-id-count` variable can take on values from ##000000–##FFFFFF, where ## represents the eight bits that are reserved for the unique identifier variable.

The `acct-session-id-count` and `acct-session-id` variables are concatenated before being sent to the RADIUS server, resulting in the accounting session being represented by the following 56-bit variable:

```
##000000 00000000–##FFFFFF FFFFFFFF
```

Examples

The following example shows how to enable the acct-session-id-count variable and sets the unique identifier variable to 5:

```
radius-server unique-ident 5
```

radius-server vsa disallow unknown

To configure the IOS to deny access when the RADIUS server returns unknown Vendor-Specific Attributes (VSAs) in its Access-Accept attribute, use the **radius-server vsa disallow unknown** command in global configuration mode.

To permit access when the RADIUS server sends unknown VSAs, use the **no** form of this command.

radius-server vsa disallow unknown

no radius-server vsa disallow unknown

Command Default Not enabled

Command Modes Global configuration: Router(config)#

Command History	Release	Modification
	12.2(4)T	This command was introduced.

Usage Guidelines It is suggested that unknown VSAs should be ignored by RADIUS clients. If an Access-Accept attribute is received that includes an attribute of unknown type, then a RADIUS client can assume that it is a potential service definition, and treat it as an Access-Reject attribute. However, there may be interoperability issues with the above suggestion, and this is why the **no** form of this command may be used in certain scenarios to configure the IOS to permit access when the RADIUS server sends unknown VSAs.

Related Commands	Command	Description
	radius-server vsa send	Configures the network access server (NAS) to recognize and use VSAs.

radius-server vsa send

To configure the network access server (NAS) to recognize and use vendor-specific attributes (VSAs), 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 [3gpp2] | authentication [3gpp2] | cisco-nas-port [3gpp2]]
```

```
no radius-server vsa send [accounting [3gpp2] | authentication [3gpp2] | cisco-nas-port [3gpp2]]
```

Syntax Description	
accounting	(Optional) Limits the set of recognized VSAs to only accounting attributes.
authentication	(Optional) Limits the set of recognized VSAs to only authentication attributes.
cisco-nas-port	(Optional) Due to the Internet Engineering Task Force (IETF) requirement for including NAS port information in attribute 87 (Attr87), the Cisco NAS port is deprecated by default. However, if your servers require this information, then the cisco-nas-port keyword can be used to return the Cisco NAS port VSA.
3gpp2	(Optional) Adds Third Generation Partnership Project 2 (3gpp2) Cisco VSAs to this packet type.

Defaults Disabled

Command Modes Global configuration (config)

Command History	Release	Modification
	11.3 T	This command was introduced.
	12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. The cisco-nas-port and 3gpp2 keywords were added to provide backward compatibility for Cisco VSAs.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The IETF draft standard specifies a method for communicating vendor-specific information between the NAS and the RADIUS server by using the VSA (attribute 26). VSAs allow vendors to support their own extended attributes not suitable for general use. The **radius-server vsa send** command enables the NAS to recognize and use both accounting and authentication VSAs. Use the **accounting** keyword with the **radius-server vsa send** command to limit the set of recognized VSAs to accounting attributes only. Use the **authentication** keyword with the **radius-server vsa send** command to limit the set of recognized VSAs to authentication attributes only.

The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. The Cisco 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 *
```

In the preceding example, “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 solution allows the full set of features available for TACACS+ authorization to also be used for RADIUS.

For example, the following AV pair causes the Cisco “multiple named ip address pools” feature to be activated during IP authorization (during the PPP Internet Protocol Control Protocol (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, see RFC 2138, *Remote Authentication Dial-In User Service (RADIUS)*.

Examples

The following example configures the NAS 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.

rate-limit (firewall)

To limit the number of Layer 7 Session Initiation Protocol (SIP) or H.323 protocol messages that strike the Cisco IOS firewall every second, use the **rate-limit** command in policy-map-class configuration mode. To remove the rate limit from the configuration, use the **no** form of this command.

rate-limit *limit-number*

no rate-limit *limit-number*

Syntax Description

<i>limit-number</i>	Number of application messages allowed per second. Range: 1 to 2147483647.
---------------------	--

Command Default

No rate limit is configured.

Command Modes

Policy-map-class configuration (config-pmap-c)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	Support for the H.323 protocol was introduced.

Usage Guidelines

Use this command when configuring a rate-limiting mechanism to monitor the call attempt rate and the number of calls per second for the H.323 or SIP protocol.

The **rate-limit** command is used with the **policy-map type inspect** command and must be configured with the **class type inspect** command.

When configuring a rate-limiting mechanism for the H.323 or SIP protocol, the **rate-limit** command is used with the appropriate **match** command to choose the required control messages. For the H.323 protocol, the **rate limit** command is used with the **match message** command. For the SIP protocol, the **rate limit** command is used with the **match request** command.

Examples

The following example configures a rate limiting mechanism of 5 invite messages per second for the SIP class map “my_sip_rt_msgs”:

```
class-map type inspect sip match-any my_sip_rt_msgs
  match request method invite
  policy-map type inspect sip my_sip_policy
  class type inspect sip my_sip_rt_msgs
  rate-limit 5
```

The following example configures a rate-limiting mechanism of 16 setup messages per second to monitor the call attempt rate for H.323 protocol based calls:

```
class-map type inspect h323 match-any my_h323_rt_msgs
  match message setup
  policy-map type inspect h323 my_h323_policy
  class type inspect h323 my_h323_rt_msgs
  rate-limit 16
```

Related Commands

Command	Description
class type inspect	Specifies the class on which an action is to be performed.
match message	Configures the match criterion for a class map on the basis of H.323 protocol messages.
policy-map type inspect	Creates an inspect type policy map.