

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.

Defaults

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.

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, which waits until the traffic is about to leave the network before filtering occurs.

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 = "cisco"
    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.

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 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

<i>format</i>	(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.

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.

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.

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	<code>vrf vrf-name</code>	(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.

Usage Guidelines	<p>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.</p> <p>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.</p>
------------------	---

Examples	<p>The following example shows a configuration that sends RADIUS attribute 44 in access-request packets:</p> <pre>aaa new-model aaa authentication ppp default group radius radius-server host 10.100.1.34 radius-server attribute 44 include-in-access-req</pre>
----------	---

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.

Defaults This command is not enabled.

Command Modes Global configuration

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

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.

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.

Defaults

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.

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 support-multiple
```

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

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

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.

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.

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 (async1-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 async1-pool
!
ip local pool async1-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 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.

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 1.1.1.1
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 1.1.1.1 key mykey1
Router(config)# radius-server attribute list usage-only
Router(config-radius-attr1)# attribute 1,40,42-43,46
Router(config-radius-attr1)# exit
Router(config)# radius-server attribute list bad-author
Router(config-radius-attr1)# 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 select the NAS-Port format used for RADIUS accounting features, and to restore the default NAS-Port format, use the **radius-server attribute nas-port format** command in global configuration mode. To stop sending attribute 5 (NAS-Port) to the RADIUS server, use the **no** form of this command.

radius-server attribute nas-port format *format*

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

Syntax Description

<i>format</i>	NAS-Port format. Possible values for the format argument are as follows:
	a —Standard NAS-Port format
	b —Extended NAS-Port format
	c —Carrier-based format
	d —PPPoX (PPP over Ethernet or PPP over ATM) extended NAS-Port format
	e —Configurable NAS-Port format

Defaults

Standard NAS-Port format

Command Modes

Global configuration

Command History

Release	Modification
11.3(7)T	This command was introduced.
11.3(9)DB	The PPP extended NAS-Port format was added.
12.1(5)T	The PPP extended NAS-Port format was expanded to support PPPoE over ATM and PPPoE over IEEE 802.1Q virtual LANS (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.

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 PPP over ATM and PPPoE over ATM, and the interface and VLAN ID for PPPoE over Institute of IEEE standard 802.1Q VLANs.

Format e

The currently supported formats **a** through **c** do not work with new 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 **x**, will provide a larger available range of values to be stored. Thus, the ranges may be expanded as follows:

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

and so on.

It is imperative that one know what the valid range is for a given parameter on a platform that one wishes to support. The IOS RADIUS client will bitmask the determined value to the maximum permissible value on the basis of configuration. Thus, 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, one must always configure enough bits to correctly capture the value required. Care must be taken to ensure that format **e** is configured to properly work for all NAS port types within your network environment.

Currently supported parameters and their representative characters are shown below.

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

PPPoX VPI	I
PPPoX VCI	C
Session ID	U

All 32 bits that represent the NAS-Port must be set to one of the above characters because this format makes no assumptions for empty fields.

Access Router

The DS0 port on a T1-based card and on a T3-based card will give different results. On T1-based cards, the physical port is equal to the virtual port (as these are the same). So, **p** and **d** will give the same information for a T1 card. However, on a T3 system, the port will give you the physical port number (as there can be more than one T3 card for a given platform). As such, **d** will give you the virtual T1 line (as per configuration on a T3 controller). On a T3 system, **p** and **d** will be different, and one should capture both to properly identify the physical device. As a working example for the Cisco AS5400, the following configuration is recommended:

```
Router (config)# radius-server attribute nas-port format e
SSSSPPPPPPPPSSSSppppppdddddccccc
```

This will give one an asynchronous slot (0 – 16), asynchronous port (0 – 512), DS0 slot (0 – 16), DS0 physical port (0 – 32), DS0 virtual port (0 – 32), and channel (0 – 32). The parser has been implemented to explicitly require 32-bit support, or it will fail.

Finally, format **e** is supported for channel-associated signaling (CAS), Primary Rate Interface (PRI), and basic rate interface- (BRI-) based interfaces.



Note

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

Examples

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

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

Related Commands

Command	Description
vpdn aaa attribute nas-port vpdn-nas	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 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.

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.

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 packet 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>

Defaults

If the *seconds* argument is not configured, the number of seconds will range from 10 to 60 seconds, depending on the transaction rate of the server.

If the *number-of-tries* 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.

Command Modes

Global configuration

Command History

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

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 indicated, both time and tries will be set to their defaults.
- If either the *seconds* or the *number-of-tries* arguments is indicated, the one indicated (time or tries) will be set to its default. The other will be unchanged.
- If both the *seconds* and the *number-of-tries* arguments are indicated, both time and tries will be set to their defaults.

Examples

The following example shows that the router will be considered dead after 5 seconds and four tries:

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

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

radius-server deadtime *minutes*

no radius-server deadtime

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.

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.

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

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

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

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



Note

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

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

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

■ radius-server directed-request

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

radius-server domain-stripping

To configure a router to strip the domain name from the username before forwarding the username to the RADIUS server, use the **radius-server domain-stripping** command in global configuration mode. To disable domain stripping, use the **no** form of this command.

```
radius-server domain-stripping [right-to-left] [delimiter character[character2...character7]]
[vrf vrf-name]
```

```
no radius-server domain-stripping [right-to-left] [delimiter character[character2...character7]]
[vrf vrf-name]
```

Syntax Description		
right-to-left		(Optional) Specifies that the domain string will be terminated at the first delimiter parsed from right to left. The default is to terminate the string at the first delimiter parsed from left to right.
delimiter <i>character</i> [<i>character2...character7</i>]		(Optional) Specifies the character or characters that will be recognized as a 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 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 delimiter is the @ character.
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 Domain stripping is disabled. The entire 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.

Usage Guidelines Use the **radius-server domain-stripping** command 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 string 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 domain information at either delimiter. For example, if the username is user@cisco.com@cisco.net, the username could be stripped in two ways. The default direction (left to right) would result in the username “user” being forwarded. Configuring the **right-to-left** keyword would result in the username “user@cisco.com” being forwarded.

Use the **delimiter** keyword to specify the character or characters that will be recognized as a delimiter. The first configured character that is parsed will be used as the delimiter.

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

Examples

The following example configures the router to parse the username from right to left and sets the valid delimiter characters as @, \, and \$:

```
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:

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

Related Commands

Command	Description
ip vrf	Defines a VRF instance and enters VRF configuration mode.

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.

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

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

Syntax Description

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

Defaults

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

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

```
radius-server host host1
```

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

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

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

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

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

To use separate servers for accounting and authentication, use the zero port value as appropriate.

The following example specifies that RADIUS server *host1* be used for accounting but not for authentication, and that RADIUS server *host2* be used for authentication but not for accounting:

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

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

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

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication ppp	Specifies one or more AAA authentication method for use on serial interfaces running PPP.
aaa authorization	Sets parameters that restrict network access to a user.
ppp	Starts an asynchronous connection using PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are selected on the interface.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server retransmit	Specifies how many times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
radius-server timeout	Sets the interval a router waits for a server host to reply.
username	Establishes a username-based authentication system, such as PPP CHAP and PAP.

radius-server host non-standard

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

radius-server host {*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.

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 <i>string</i> • 7 <i>string</i> • <i>string</i>

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 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 Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples

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

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

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.
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.

Command	Description
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.

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 default is 3 attempts.				
Defaults	3 attempts				
Command Modes	Global configuration				
Command History	<table><thead><tr><th>Release</th><th>Modification</th></tr></thead><tbody><tr><td>11.1</td><td>This command was introduced.</td></tr></tbody></table>	Release	Modification	11.1	This command was introduced.
Release	Modification				
11.1	This command was introduced.				
Usage Guidelines	The Cisco IOS software tries all servers, allowing each one to time out before increasing the retransmit count.				
Examples	The following example specifies a retransmit counter value of five times: <pre>radius-server retransmit 5</pre>				

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(27)SB	This command was integrated into Cisco IOS Release 12.2(27)SB.

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:

```
Router (config)# aaa new-model
radius-server retry method reorder
radius-server retransmit 0
radius-server transaction max-tries 6
radius-server host 1.2.3.4 key rad123
radius-server host 4.5.6.7 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 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 default is 5 seconds.
--------------------	----------------	---

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

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

Command History	Release	Modification
	11.1	This command was introduced.

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

Examples	The following example changes the interval timer to 10 seconds:
----------	---

```
radius-server timeout 10
```

Related Commands	Command	Description
	radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.	

radius-server 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	<i>number</i>	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(27)SB	This command was integrated into Cisco IOS Release 12.2(27)SB.

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 1.2.3.4
radius-server host 5.6.7.8
```

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 acct-session-id-count 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 send

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

radius-server vsa send [accounting | authentication]

no radius-server vsa send [accounting | authentication]

Syntax Description

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

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

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

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

The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. Cisco's vendor-ID is 9, and the supported option has vendor-type 1, which is named "cisco-avpair." The value is a string with the following format:

```
protocol : attribute sep value *
```

"Protocol" is a value of the Cisco "protocol" attribute for a particular type of authorization. "Attribute" and "value" are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification, and "sep" is "=" for mandatory attributes and "*" for optional attributes. This allows the full set of features available for TACACS+ authorization to also be used for RADIUS.

For example, the following AV pair causes Cisco's "multiple named ip address pools" feature to be activated during IP authorization (during PPP's IPCP address assignment):

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

The following example causes a “NAS Prompt” user to have immediate access to EXEC commands.

```
cisco-avpair= "shell:priv-lvl=15"
```

Other vendors have their own unique vendor-IDs, options, and associated VSAs. For more information about vendor-IDs and VSAs, refer to RFC 2138, *Remote Authentication Dial-In User Service (RADIUS)*.

Examples

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

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

Related Commands

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

reauthentication time

To enter the time limit after which the authenticator should reauthenticate, use the **reauthentication time** command in local RADIUS server group configuration mode. To remove the requirement that users reauthenticate after the specified duration, use the **no** form of this command.

reauthentication time *seconds*

no reauthentication time *seconds*

Syntax Description

<i>seconds</i>	Number of seconds after which reauthentication occurs.
----------------	--

Defaults

The default setting is 0 seconds, which means that group members are not required to reauthenticate.

Command Modes

Local RADIUS server group configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples

The following example shows that the time limit after which the authenticator should reauthenticate is 30 seconds:

```
reauthentication time 30
```

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.
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.

Command	Description
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
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.

redirect (identity policy)

To redirect clients to a particular URL, use the **redirect** command in identity policy configuration mode. To remove the URL, use the **no** form of this command.

redirect url *url*

no redirect url *url*

Syntax Description

url	URL to which clients should be redirected.
<i>url</i>	Valid URL.

Defaults

No default behavior or values

Command Modes

Identity policy configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

When you use this command, an identity policy has to be associated with an Extensible Authentication Protocol over UDP (EAPoUDP) identity profile.

Examples

The following example shows the URL to which clients will be redirected:

```
Router (config)# identity policy p1
Router (config-identity-policy)# redirect url http://www.cisco.com
```

Related Commands

Command	Description
identity policy	Creates an identity policy.

redundancy stateful

To configure stateful failover for tunnels using IP Security (IPSec), use the **redundancy stateful** command in crypto map configuration mode. To disable stateful failover for tunnel protection, use the **no** form of this command.

redundancy *standby-group-name* **stateful**

no redundancy *standby-group-name* **stateful**

Syntax Description

<i>standby-group-name</i>	Refers to the name of the standby group as defined by Hot Standby Router Protocol (HSRP) standby commands. Both routers in the standby group are defined by this argument and share the same virtual IP (VIP) address.
---------------------------	--

Defaults

Stateful failover is not enabled for IPSec tunnels.

Command Modes

Crypto map configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

The **redundancy stateful** command uses an existing IPSec profile (which is specified via the **crypto ipsec profile** command) to configure IPSec stateful failover for tunnel protection. (You do not configure the tunnel interface as you would with a crypto map configuration.) IPSec stateful failover enables you to define a backup IPSec peer (secondary) to take over the tasks of the active (primary) router if the active router is deemed unavailable.

The tunnel source address must be a VIP address, and it must not be an interface name.

Examples

The following example shows how to configure stateful failover for tunnel protection:

```
crypto ipsec profile peer-profile
  redundancy HA-out stateful

interface Tunnel1
 ip unnumbered Loopback0
 tunnel source 209.165.201.3
 tunnel destination 10.0.0.5
 tunnel protection ipsec profile peer-profile
!
interface Ethernet0/0
 ip address 209.165.201.1 255.255.255.224
 standby 1 ip 209.165.201.3
 standby 1 name HA-out
```

■ redundancy stateful

Related Commands

Command	Description
crypto ipsec profile	Defines the IPSec parameters that are to be used for IPSec encryption between two routers and enters crypto map configuration mode.

regenerate

To enable key rollover with manual certificate enrollment, use the **regenerate** command in ca-trustpoint configuration mode. To disable key rollover, use the **no** form of this command.

regenerate

no regenerate

Syntax Description

This command has no arguments or keywords.

Defaults

Key rollover is not enabled.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use the **regenerate** command to provide seamless key rollover for manual certificate enrollment. A new key pair is created with a temporary name, and the old certificate and key pair are retained until a new certificate is received from the certification authority (CA). When the new certificate is received, the old certificate and key pair are discarded and the new key pair is renamed with the name of the original key pair.

If the key pair being rolled over is exportable, the new key pair will also be exportable. The following comment will appear in the trustpoint configuration to indicate whether the key pair is exportable:

```
! RSA keypair associated with trustpoint is exportable
```

Do not regenerate the keys manually; key rollover will occur when the **crypto ca enroll** command is issued.

Examples

The following example shows how to configure key rollover to regenerate new keys with a manual certificate enrollment from the CA named "trustme2".

```
crypto ca trustpoint trustme2
 enrollment url http://trustme2.company.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet0
 serial-number none
 regenerate
 password revokeme
 rsakeypair trustme2 2048
 exit
crypto ca authenticate trustme2
crypto ca enroll trustme2
```

Related Commands

Command	Description
crypto ca authenticate	Retrieves the CA certificate and authenticates it.
crypto ca enroll	Requests certificates from the CA for all of your router's RSA key pairs.
crypto ca trustpoint	Declares the CA that your router should use.

request-method

To permit or deny HTTP traffic according to either the request methods or the extension methods, use the **request-method** command in appfw-policy-http configuration mode. To disable this inspection parameter, use the **no** form of this command.

```
request-method { rfc rfc-method | extension extension-method } action { reset | allow } [alarm]
```

```
no request-method { rfc rfc-method | extension extension-method } action { reset | allow } [alarm]
```

Syntax Description

rfc	Specifies that the supported methods of RFC 2616, <i>Hypertext Transfer Protocol—HTTP/1.1</i> , are to be used for traffic inspection.
<i>rfc-method</i>	Any one of the following RFC 2616 methods can be specified: connect , default , delete , get , head , options , post , put , trace .
extension	Specifies that the extension methods are to be used for traffic inspection.
<i>extension-method</i>	Any one of the following extension methods can be specified: copy , default , edit , getattribute , getproperties , index , lock , mkdir , move , revadd , relabel , revlog , save , setattribute , startrev , stoprev , unedit , unlock .
action	Methods and extension methods outside of the specified method are subject to the specified action (reset or allow).
reset	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
allow	Forwards the packet through the firewall.
alarm	(Optional) Generates system logging (syslog) messages for the given action.

Defaults

If a given method is not specified, all methods and extension methods are supported with the reset alarm action.

Command Modes

appfw-policy-http configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Only methods configured by the **request-method** command are allowed through the firewall; all other HTTP traffic is subjected to the specified action (**reset** or **allow**).

Examples

The following example shows how to define the HTTP application firewall policy “mypolicy.” This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule “firewall,” which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
```

```
application http
strict-http action allow alarm
content-length maximum 1 action allow alarm
content-type-verification match-req-rsp action allow alarm
max-header-length request 1 response 1 action allow alarm
max-uri-length 1 action allow alarm
port-misuse default action allow alarm
request-method rfc default action allow alarm
request-method extension default action allow alarm
transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

reverse-route

To create source proxy information for a crypto map entry, use the **reverse-route** command in crypto map configuration mode. To remove the source proxy information from a crypto map entry, use the **no** form of this command.

```
reverse-route [[static] | tag {tag-id} [static] | remote-peer [static] | remote-peer {ip-address}
[static]]
```

```
no reverse-route [[static] | tag {tag-id} [static] | remote-peer [static] | remote-peer [ip-address]
[static]]
```

Syntax Description

static	(Optional) Creates routes according to the existence of crypto access control lists (ACLs).
tag {tag-id}	Tag value that can be used as a “match” value for controlling redistribution via route maps.
remote-peer [static]	Two routes are created, one for the remote endpoint and one for route recursion to the remote endpoint via the interface to which the crypto map is applied. <ul style="list-style-type: none"> The static keyword is optional.
remote-peer {ip-address} [static]	One route is created to a remote proxy by way of a user-defined next hop. This next hop can be used to override a default route. <ul style="list-style-type: none"> The <i>ip-address</i> argument is required. The static keyword is optional.

Defaults

No default behavior or values.

Command Modes

Crypto map configuration

Command History

Release	Modification
12.1(9)E	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(11)T	This command was implemented on the Cisco AS5300 and Cisco AS5800 platforms.
12.2(13)T	The remote-peer keyword and <i>ip-address</i> argument were added.
12.3(14)T	The static and tag keywords and <i>tag-id</i> argument were added.

Usage Guidelines

This command can be applied on a per-crypto map basis.

Reverse route injection (RRI) provides a scalable mechanism to dynamically learn and advertise the IP address and subnets that belong to a remote site that connects through an IP Security (IPSec) Virtual Private Network (VPN) tunnel.

When enabled in an IPsec crypto map, RRI will learn all the subnets from any network that is defined in the crypto ACL as the destination network. The learned routes are installed into the local routing table as static routes that point to the encrypted interface. When the IPsec tunnel is torn down, the associated static routes will be removed. These static routes may then be redistributed into other dynamic routing protocols so that they can be advertised to other parts of the network (usually done by redistributing RRI routes into dynamic routing protocols on the core side).

Examples

Prior to Cisco IOS Release 12.3(14)T

The following is an example in which RRI has been configured when crypto ACLs exist. The example shows that all remote VPN gateways connect to the router via 192.168.0.3. RRI is added on the static crypto map, which creates routes on the basis of the source network and source netmask that are defined in the crypto ACL.

```
crypto map mymap 1 ipsec-isakmp
  set peer 10.1.1.1
  reverse-route
  set transform-set esp-3des-sha
  match address 102
```

```
Interface FastEthernet 0/0
ip address 192.168.0.2 255.255.255.0
standby name group1
standby ip 192.168.0.3
crypto map mymap redundancy group1
```

```
access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
```

Note that in Cisco IOS Release 12.3(14)T and later, for the static map to retain this same behavior of creating routes on the basis of crypto ACL content, the **static** keyword will be needed, that is, **reverse-route static**.

The **reverse-route** command in this situation creates routes that are analogous to the following static route command-line interface (CLI) commands (**ip route**):

- Remote Tunnel Endpoint


```
ip route 10.1.1.1 255.255.255.255 192.168.1.1
```
- VPN Services Module (VPNSM)


```
ip route 10.1.1.1 255.255.255.255 vlan0.1
```

In the following example, two routes are created, one for the remote endpoint and one for route recursion to the remote endpoint via the interface on which the crypto map is configured.

```
reverse-route remote-peer
```

Configuring RRI with the Enhancements Added in Cisco IOS Release 12.3(14)T

The following configuration example shows that RRI has been configured for a situation in which there are existing ACLs:

```
crypto map mymap 1 ipsec-isakmp
  set peer 172.17.11.1
  reverse-route static
  set transform-set esp-3des-sha
  match address 101
```

```
access-list 101 permit ip 192.168.1.0 0.0.0.255 172.17.11.0 0.0.0.255
```

The following example shows how RRI-created routes can be tagged with a tag number and then used by a routing process to redistribute those tagged routes via a route map.

```
crypto dynamic-map ospf-clients 1
  reverse-route tag 5

router ospf 109
  redistribute rip route-map rip-to-ospf

route-map rip-to-ospf permit
  match tag 5
  set metric 5
  set metric-type type1

show ip ospf topology

P 10.81.7.48/29, 1 successors, FD is 2588160, tag is 5
  via 192.168.82.25 (2588160/2585600), FastEthernet0/1
```

The following example shows that one route has been created to the remote proxy via a user-defined next hop. This next hop should not require a recursive route lookup unless it will recurse to a default route.

```
reverse-route remote-peer 10.4.4.4
```

The above example yields the following prior to Cisco IOS Release 12.3(14)T:

```
10.0.0.0/24 via 10.1.1.1 (in the VRF table if VRFs are configured)
10.1.1.1/32 via 10.4.4.4 (in the global route table)
```

And this result occurs with RRI enhancements:

```
10.0.0.0/24 via 10.4.4.4 (in the VRF table if VRFs are configured, otherwise in the global table)
```

Related Commands

Command	Description
crypto map (global IPsec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPsec traffic.
show crypto map (IPsec)	Displays the crypto map configuration.

revocation-check

To check the revocation status of a certificate, use the **revocation-check** command in ca-trustpoint configuration mode. To disable this functionality, use the **no** form of this command.

```
revocation-check method1 [method2[method3]]
```

```
no revocation-check method1 [method2[method3]]
```

Syntax Description

<i>method1</i> [<i>method2</i> [<i>method3</i>]]	Method used by the router to check the revocation status of the certificate. Available methods are as follows: <ul style="list-style-type: none"> • cr1—Certificate checking is performed by a certificate revocation list (CRL). This is the default behavior. • none—Certificate checking is not required. • ocsp—Certificate checking is performed by an online certificate status protocol (OCSP) server. <p>If a second and third method are specified, each method will be used only if the previous method returns an error, such as a server being down.</p>
--	--

Defaults

After a trustpoint is enabled, the default is set to **revocation-check cr1**, which means that CRL checking is mandatory.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(2)T	This command was introduced. This command replaced the cr1 best-effort and cr1 optional commands.

Usage Guidelines

Use the **revocation-check** command to specify at least one method that is to be used to ensure that the certificate of a peer has not been revoked.

If your router does not have the applicable CRL and is unable to obtain one or if the OCSP server returns an error, your router will reject the peer's certificate—unless you include the **none** keyword in your configuration. If the **none** keyword is configured, a revocation check will not be performed and the certificate will always be accepted. If the **revocation-check none** command is configured, you cannot manually download the CRL via the **crypto pki cr1 request** command because the manually downloaded CRL may not be deleted after it expires. The expired CRL can cause all certificate verifications to be denied.



Note

The **none** keyword replaces the **optional** keyword that is available from the **cr1** command. If you enter the **cr1 optional** command, it will be written back as the **revocation-check none** command. However, there is a difference between the **cr1 optional** command and the **revocation-check none** command. The **cr1 optional** command will perform revocation checks against any applicable in-memory CRL. If a CRL

is not available, a CRL will not be downloaded and the certificate is treated as valid; the **revocation-check none** command ignores the revocation check completely and always treats the certificate as valid.

Also, the **crl** and **none** keywords issued together replace the **best-effort** keyword that is available from the **crl** command. If you enter the **crl best-effort** command, it will be written back as the **revocation-check crl none** command.

Examples

The following example shows how to configure the router to use the OCSP server that is specified in the AIA extension of the certificate:

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check ocs
```

The following example shows how to configure the router to download the CRL from the CDP; if the CRL is unavailable, the OCSP server that is specified in the Authority Info Access (AIA) extension of the certificate will be used. If both options fail, certificate verification will also fail.

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check crl ocs
```

The following example shows how to configure your router to use the OCSP server at the HTTP URL “http://myocspserver:81.” If the server is down, revocation check will be ignored.

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# ocs url http://myocspserver:81
Router(ca-trustpoint)# revocation-check ocs none
```

Related Commands

Command	Description
crl query	Queries the CRL to ensure that the certificate of the peer has not been revoked.
crypto pki trustpoint	Declares the CA that your router should use.
ocs url	Enables an OCSP server.

root

To obtain the certification authority (CA) certificate via TFTP, use the **root** command in ca-trustpoint configuration mode. To deconfigure the CA, use the **no** form of this command.

```
root tftp server-hostname filename
```

```
no root tftp server-hostname filename
```

Syntax Description

tftp	Defines the TFTP protocol to get the root certificate.
<i>server-hostname</i>	Specifies a name for the server and a name for the file that will store the trustpoint CA.
<i>filename</i>	

Defaults

A CA certificate is not configured.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

This command allows you to access the CA via the TFTP protocol, which is used to get the CA. You want to configure a CA certificate so that your router can verify certificates issued to peers. Thus, your router does not have to enroll with the CA that issued the certificates the peers.

Before you can configure this command, you must enable the **crypto ca trustpoint** command, which puts you in ca-trustpoint configuration mode.



Note

The **crypto ca trustpoint** command deprecates the **crypto ca identity** and **crypto ca trusted-root** commands and all related subcommands (all ca-identity and trusted-root configuration mode commands). If you enter a ca-identity or trusted-root subcommand, the configuration mode and command will be written back as ca-trustpoint.

Examples

The following example shows how to configure the CA certificate named “bar” using TFTP:

```
crypto ca trustpoint bar
root tftp xxx fff
crl optional
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

root CEP

The **crypto ca trustpoint** command deprecates the **crypto ca trusted-root** command and all related subcommands (all trusted-root configuration mode commands). If you enter a trusted-root subcommand, the configuration mode and command will be written back as ca-trustpoint.

root PROXY

The **root PROXY** command is replaced by the **enrollment http-proxy** command. See the **enrollment http-proxy** command for more information.

root TFTP

The **root TFTP** command is replaced by the **root** command. See the **root** command for more information.

rsakeypair

To specify which key pair to associate with the certificate, use the **rsakeypair** command in ca-trustpoint configuration mode.

```
rsakeypair key-label [key-size [encryption-key-size]]
```

Syntax Description

<i>key-label</i>	Name of the key pair, which is generated during enrollment if it does not already exist or if the auto-enroll regenerate command is configured.
<i>key-size</i>	(Optional) Size of the desired Rivest, Shamir, Adelman (RSA) key. If not specified, the existing key size is used.
<i>encryption-key-size</i>	(Optional) Size of the second key, which is used to request separate encryption, signature keys, and certificates.

Defaults

The fully qualified domain name (FQDN) key is used.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

When you regenerate a key pair, you are responsible for reenrolling the identities associated with the key pair. Use the **rsakeypair** command to refer back to the named key pair.

Examples

The following example is a sample trustpoint configuration that specifies the RSA key pair “exampleCAkeys”:

```
crypto ca trustpoint exampleCAkeys
enroll url http://exampleCAkeys/certsrv/mscep/mscep.dll
rsakeypair exampleCAkeys 1024 1024
```

Related Commands

Command	Description
auto-enroll	Enables autoenrollment.
crl	Generates RSA key pairs.
crypto ca trustpoint	Declares the CA that your router should use.

rsa-pubkey

To define the Rivest, Shamir, and Adelman (RSA) manual key to be used for encryption or signature during Internet Key Exchange (IKE) authentication, use the **rsa-pubkey** command in keyring configuration mode. To remove the manual key that was defined, use the **no** form of this command.

```
rsa-pubkey {address address | name fqdn} [encryption | signature]
```

```
no rsa-pubkey {address address | name fqdn} [encryption | signature]
```

Syntax Description

address <i>address</i>	IP address of the remote peer.
name <i>fqdn</i>	Fully qualified domain name (FQDN) of the peer.
encryption	(Optional) The manual key is to be used for encryption.
signature	(Optional) The manual key is to be used for signature.

Defaults

No default behavior or values

Command Modes

Keyring configuration

Command History

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

Usage Guidelines

Use this command to enter public key chain configuration mode. Use this command when you need to manually specify RSA public keys of other IP Security (IPSec) peers. You need to specify the keys of other peers when you configure RSA encrypted nonces as the authentication method in an IKE policy at your peer router.

Examples

The following example shows that the RSA public key of an IPSec peer has been specified:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```