radius attribute nas-port-type through rd

radius-server attribute nas-port format

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

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

radius-server attribute nas-port format *format*

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

Extended NAS-Port Support

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

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

Syntax Description

format	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--C onfigurable NAS-Port format
string	(Optional) Represents all of a specific port typefor format e. It is possible to specify multiple values with this argument.
type *nas-port-type*	(Optional) Allows you to globally specify different format strings to represent specific physical port types. You may set one of the extended NAS-Port-Type attribute values: • **type 30** --PPP over ATM (PPPoA) • **type 31** --PPP over Ethernet (PPPoE) over ATM (PPPoEoA) • **type 32** --PPPoE over Ethernet (PPPoEoE) • **type 33** --PPPoE over VLAN (PPPoEoVLAN) • **type 34** --PPPoE over Q-in-Q (PPPoEoQinQ)

Command Default

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

Command Modes

Global configuration

Command History

Release	Modification
11.3(7)T	This command was introduced.
11.3(9)DB	The PPP extended NAS-Port format was added.
12.1(5)T	The PPP extended NAS-Port format was expanded to support PPPoE over ATM and PPPoE over IEEE 802.1Q VLANs.
12.2(4)T	Format e was introduced.
12.2(11)T	Format e was extended to support PPPoX information.
12.3(3)	Format e was extended to support Session ID U.
12.3(7)XI1	Format e was extended to allow the format string to be NAS-Port-Type attribute specific. The following keyword and arguments were added: *string,* **type** *nas-port-type.*
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

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

The following NAS-Port formats are supported:

- Standard NAS-Port format--This 16-bit NAS-Port format indicates the type, port, and channel of the controlling interface. This is the default format used by Cisco IOS software.
- Extended NAS-Port format--The standard NAS-Port attribute field is expanded to 32 bits. The upper 16 bits of the NAS-Port attribute display the type and number of the controlling interface; the lower 16 bits indicate the interface that is undergoing authentication.

- Shelf-slot NAS-Port format--This 16-bit NAS-Port format supports expanded hardware models requiring shelf and slot entries.
- PPP extended NAS-Port format--This NAS-Port format uses 32 bits to indicate the interface, virtual path identifier (VPI), and virtual channel indicator (VCI) for PPPoA and PPPoEoA, and the interface and VLAN ID for PPPoE over Institute of Electrical and Electronic Engineers (IEEE) standard 802.1Q VLANs.

Format e

Before Cisco IOS Release 12.2(4)T formats a through c did not work with Cisco platforms such as the AS5400. For this reason, a configurable format e was developed. Format e requires you to explicitly define the usage of the 32 bits of attribute 25 (NAS-Port). The usage is defined with a given parser character for each NAS-Port field of interest for a given bit field. By configuring a single character in a row, such as x, only one bit is assigned to store that given value. Additional characters of the same type, such as x, will provide a larger available range of values to be stored. The table belowshows how the ranges may be expanded:

Table 1: Format e Ranges

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

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

The table below shows the supported parameters and their characters:

Table 2: Supported Parameters and Characters

Supported Parameters	Characters
Zero	0 (always sets a 0 to that bit)
One	1 (always sets a 0 to that bit)
DS0 shelf	f
DS0 slot	s

Supported Parameters	Characters
DS0 adaptor	a
DS0 port	p (physical port)
DS0 subinterface	i
DS0 channel	c
Async shelf	F
Async slot	S
Async port	P
Async line	L (modern line number, that is, physical terminal [TTY] number)
PPPoX slot	S
PPPoX adaptor	A
PPPoX port	P
PPPoX VLAN ID	V
PPPoX VPI	I
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 (because 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 (because 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 SSSSPPPPPPPPPssssppppccccc
```

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), PRI, and BRI-based interfaces.

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

Extended NAS-Port-Type Attribute Support

This command allows you to configure a specific service port type for extended attribute 61 support which overrides the default global setting.

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

The following example shows how to configure global support for extended NAS-Port-Type ports and how to specify two separate format e strings globally for two different types of ports:

- type 30 (which is PPPoA)
- type 33 which is (PPPoEoVLAN)

```
Router# configure terminal
Router(config)#
Router(config)# radius-server attribute 61 extended
Router(config)# radius-server attribute nas-port format e SSSSAPPPUUUUUUUUUUUUUUUUUUUUUUUU
Router(config)# radius-server attribute nas-port format e SSSSAPPPIIIIIIIICCCCCCCCCCCCCCCC
 type 30

Router(config)#
Router(config)# radius-server attribute nas-port format e SSSSAPPPVVVVVVVVVVVVVVVVVVVVVVVV
 type 33
```

Related Commands

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

radius-server 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.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **radius-server configure-nas** command to have the Cisco router query the vendor-proprietary RADIUS server for static routes and IP pool definitions when the router first starts up. Some vendor-proprietary implementations of RADIUS let the user define static routes and IP pool definitions on the RADIUS server instead of on each individual network access server in the network. As each network access server starts up, it queries the RADIUS server for static route and IP pool information. This command enables the Cisco router to obtain static routes and IP pool definition information from the RADIUS server.

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

Examples

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

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

Related Commands

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

radius-server dead-criteria

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

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

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

Syntax Description

time *seconds*	(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. • 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. **Note** Both the time criterion and the tries criterion must be met for the server to be marked as dead.
tries *number-of-tries*	(Optional) Number of consecutive timeouts that must occur on the router before the RADIUS server is marked as dead. If the server performs both authentication and accounting, both types of packets will be included in the number. Improperly constructed packets will be counted as though they were timeouts. All transmissions, including the initial transmit and all retransmits, will be counted. You can configure the number of timeouts to be from 1 through 100. • 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. **Note** Both the time criterion and the tries criterion must be met for the server to be marked as dead.

Command Default

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

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

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

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

Examples

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

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

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

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

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

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

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

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

Related Commands

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

radius-server deadtime

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

radius-server deadtime *minutes*

no radius-server deadtime

Syntax Description

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

Command Default

Dead time is set to 0.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

Use this command to enable 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 specified duration (in minutes) or unless there are no servers not marked as “dead.”

Note If a RADIUS server that is marked as “dead” receives a directed-request, the directed- request is not omitted by the RADIUS server. The RADIUS server continues to process the directed-request because the request is directly sent to the RADIUS server.

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 packet 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. At at least the requisite number of retransmits plus one (for the initial transmission) have been sent consecutively across all transactions being sent to the RADIUS server without receiving a valid response from the server within the requisite timeout.

Examples

The following example specifies five minutes of 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 that 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 host

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

Cisco IOS Release 12.4T and Later Releases

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

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

All Other Releases

radius-server host {*hostname*| *ip-address*} [**alias**{*hostname*| *ip-address*}| [**acct-port** *port-number*] [**auth-port** *port-number*] **[non-standard]** [**timeout** *seconds*] [**retransmit** *retries*] [**test username** *user-name* **[ignore-acct-port] [ignore-auth-port]** [**idle-time** *minutes*]] [**backoff exponential** [**max-delay** *minutes*] [**backoff-retry** *number-of-retransmits*]] [**key-wrap encryption-key** *encryption-key* **message-auth-code-key** *encryption-key* [**format** {**ascii**| **hex**}]| **pac**] [**key** *encryption-key*]]

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

Syntax Description

hostname	Domain Name System (DNS) name of the RADIUS server host.
ip-address	IP address of the RADIUS server host.
alias	(Optional) Allows up to eight aliases per line for any given RADIUS server.
acct-port *port-number*	(Optional) UDP destination port for accounting requests. • The host is not used for authentication if the port number is set to zero. If the port number is not specified, the default port number assigned is 1646.
auth-port *port-number*	(Optional) UDP destination port for authentication requests. • The host is not used for authentication if the port number is set to zero. If the port number is not specified, the default port number assigned is 1645.
non-standard	Parses attributes that violate the RADIUS standard.

timeout *seconds*	(Optional) Time interval (in seconds) that the device waits for the RADIUS server to reply before retransmitting. • The timeout keyword overrides the global value of the **radius-server timeout** command. • If no timeout value is specified, a global value is used; the range is from 1 to 1000.
retransmit *retries*	(Optional) Number of times a RADIUS request is resent to a server, if that server is not responding or there is a delay in responding. • The retransmit keyword overrides the global setting of the **radius-server retransmit** command. • If no retransmit value is specified, a global value is used; the range is from 1 to 100.
test username *user-name*	(Optional) Sets the test username for the automated testing feature for RADIUS server load balancing.
ignore-acct-port	(Optional) Disables the automated testing feature for RADIUS server load balancing on the accounting port.
ignore-auth-port	(Optional) Disables the automated testing feature for RADIUS server load balancing on the authentication port.
idle-time *minutes*	(Optional) Length of time (in minutes) the server remains idle before it is quarantined and test packets are sent out. The range is from 1 to 35791. The default is 60.
backoff exponential	(Optional) Sets the exponential retransmits backup mode.
max-delay *minutes*	(Optional) Sets the maximum delay (in minutes) between retransmits. • **max-delay** *minutes* *minutes*—The range is from 1 to 120. The default value is 3.
key-wrap encryption-key	(Optional) Specifies the key-wrap encryption key.

message-auth-code-key	Specifies the key-wrap message authentication code key.
format	(Optional) Specifies the format of the message authenticator code key. • Valid values are: ◦ **ascii—**Configures the key in ASCII format. ◦ **hex—**Configures the key in hexadecimal format.
backoff-retry *number-of-retransmits*	(Optional) Specifies the exponential backoff retry. • *number-of-retransmits*—Number of backoff retries. The range is from 1 to 50. The default value is 8.
pac	(Optional) Generates the per-server Protected Access Credential (PAC) key.
key	(Optional) Encryption key used between the device and the RADIUS daemon running on this RADIUS server. • The **key** keyword overrides the global setting of the **radius-server key** command. If no key string is specified, a global value is used. **Note** The **key** keyword 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 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.
encryption-key	Specifies the encryption key. • Valid values for *encryption-key* are: ◦ **0—**Specifies that an unencrypted key follows. ◦ **7—**Specifies that a hidden key follows. ◦ String specifying the unencrypted (clear-text) server key.

Command Default

No RADIUS host is specified and RADIUS server load balancing automated testing is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.0(5)T	This command was modified to add options for configuring timeout, retransmission, and key values per RADIUS server.
12.1(3)T	This command was modified. The **alias** keyword was added.
12.2(15)B	This command was integrated into Cisco IOS Release 12.2(15)B. The **backoff exponential**, **backoff-retry**, **key**, and **max-delay** keywords and *number-of-retransmits, encryption-key*, and *minutes* arguments were added.
12.2(28)SB	This command was integrated into Cisco release 12.2(28)SB. The **test username** *user-name*, **ignore-auth-port**, **ignore-acct-port**, and **idle-time** *seconds* keywords and arguments were added for configuring the RADIUS server load balancing automated testing functionality.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. The keywords and arguments that were added in Cisco IOS Release 12.2(28)SB apply to Cisco IOS Release 12.2(33)SRA and subsequent 12.2SR releases.
12.4(11)T	This command was modified. **Note** The keywords and arguments that were added in Cisco IOS Release 12.2(28)SB do not apply to Cisco IOS Release 12.4(11)T or to subsequent 12.4T releases.
12.2 SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. **Note** The keywords and arguments that were added in Cisco IOS Release 12.2(28)SB do not apply to Cisco IOS Release 12.2SX.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.3(1)S	This command was modified. The **key-wrap encryption-key**, **message-auth-code-key**, **format**, **ascii**, and **hex** keywords were added.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

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.

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

If you configure one RADIUS server with a nonstandard option and another RADIUS server without the nonstandard option, the RADIUS server host with the nonstandard option does not accept a predefined host. However, if you configure the same RADIUS server host IP address for different UDP destination ports, where one UDP destination port (for accounting requests) is configured using the **acct-port** keyword and another UDP destination port (for authentication requests) is configured using the **auth-port** keyword with and without the nonstandard option, the RADIUS server does not accept the nonstandard option. This results in resetting all the port numbers. You must specify a host and configure accounting and authentication ports on a single line.

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

RADIUS Server Automated Testing

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

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

Examples

The following example shows how to specify host1 as the RADIUS server and to use default ports for both accounting and authentication depending on the Cisco release that you are using:

```
radius-server host host1
```

The following example shows how to specify 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 shows how to specify the host with IP address 192.0.2.46 as the RADIUS server, uses ports 1612 and 1616 as the authorization and accounting ports, sets the timeout value to six, sets the retransmit value to five, and sets “rad123” as the encryption key, thereby matching the key on the RADIUS server:

```
radius-server host 192.0.2.46 auth-port 1612 acct-port 1616 timeout 6 retransmit 5 key
rad123
```

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

The following example shows how to specify the RADIUS server host1 for accounting but not for authentication, and the RADIUS server host2 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 shows how to specify four aliases on the RADIUS server with IP address 192.0.2.1:

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

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

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

The following example shows how to configure automatic PAC provisioning on a device. In seed devices, the PAC-Opaque has to be provisioned so that all RADIUS exchanges can use this PAC-Opaque to enable automatic PAC provisioning for the server being used. All nonseed devices obtain the PAC-Opaque during the authentication phase of a link initialization.

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

Examples

The following example shows how to enable RADIUS server automated testing for load balancing with the authorization and accounting ports specified depending on the Cisco release that you are using:

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

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication ppp	Specifies one or more AAA authentication method for use on serial interfaces that run PPP.
aaa authorization	Sets parameters that restrict network access to a user.
debug aaa test	Shows when the idle timer or dead timer has expired for RADIUS server load balancing.
load-balance	Enables RADIUS server load balancing for named RADIUS server groups.
ppp	Starts an asynchronous connection using PPP.
ppp authentication	Enables CHAP or PAP or both and specifies the order in which CHAP and PAP authentication are to be selected on the interface.

Command	Description
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the device and the RADIUS daemon.
radius-server load-balance	Enables RADIUS server load balancing for the global RADIUS server group.
radius-server retransmit	Specifies the number of times Cisco software searches the list of RADIUS server hosts before giving up.
radius-server timeout	Sets the interval that a device waits for a server host to reply.
test aaa group	Tests the RADIUS load balancing server response manually.
username	Establishes a username-based authentication system, such as PPP CHAP and PAP.

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

Command Default

The authentication and encryption key is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.1(3)T	This command was modified. The *string* argument was modified as follows: • **0** *string* • **7** *string* • *string*
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

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 “key1”:

```
Router(config)# radius-server key key1
```

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.
aaa new-model	Enables AAA access control model.
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.

Command	Description
username	Establishes a username-based authentication system, such as PPP CHAP and PAP.

radius-server load-balance

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

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

no radius-server load-balance

Syntax Description

method least-outstanding	Enables least outstanding mode for load balancing.
batch-size	(Optional) The number of transactions to be assigned per batch.
number	(Optional) The number of transactions in a batch. • The default is 25. • The range is 1-2147483647. **Note** Batch size may impact throughput and CPU load. It is recommended that the default batch size, 25, be used because it is optimal for high throughput, without adversely impacting CPU load.
ignore-preferred-server	(Optional) Indicates if a transaction associated with a single AAA session should attempt to use the same server or not. • If set, preferred server setting will not be used. • Default is to use the preferred server.

Command Default

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

Command Modes

Global configuration

Command History

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

Examples

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

Examples

The following shows the relevant RADIUS configuration:

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

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

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

Examples

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

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

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

Server Status Information for Global RADIUS Server Group Example

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

```
Router# show aaa server
RADIUS:id 4, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
     State:current UP, duration 3175s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 6, timeouts 1
             Response:unexpected 1, server error 0, incorrect 0, time 1841ms
             Transaction:success 5, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 5, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 3303ms
             Transaction:success 5, failure 0
     Elapsed time since counters last cleared:2m
RADIUS:id 5, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
     State:current UP, duration 3175s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 6, timeouts 1
             Response:unexpected 1, server error 0, incorrect 0, time 1955ms
```

```
                Transaction:success 5, failure 0
        Author:request 0, timeouts 0
                Response:unexpected 0, server error 0, incorrect 0, time 0ms
                Transaction:success 0, failure 0
        Account:request 5, timeouts 0
                Response:unexpected 0, server error 0, incorrect 0, time 3247ms
                Transaction:success 5, failure 0
        Elapsed time since counters last cleared:2m
Router#
```

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

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

Related Commands

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

radius-server retransmit

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

radius-server retransmit *retries*

no radius-server retransmit

Syntax Description

retries	Maximum number of retransmission attempts. The range is 0 to 100.

Command Default

The default number of retransmission attempts is 3.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

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

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

Examples

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

```
Router(config)# radius-server retransmit 5
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server timeout	Sets the interval for which a router waits for a server host to reply.
show radius statistics	Displays the RADIUS statistics for accounting and authentication packets.

radius-server timeout

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

radius-server timeout *seconds*

no radius-server timeout

Syntax Description

seconds	Number that specifies the timeout interval, in seconds. The range is 1 to 1000. The default is 5 seconds .

Command Default

5 seconds

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

If the RADIUS server is only a few hops from the router, we recommend that you configure the RADIUS server timeout to 15 seconds.

Examples

The following example shows how to set the interval timer to 10 seconds:

```
radius-server timeout 10
```

Related Commands

Command	Description
radius-server host	Specifies a RADIUS server host.

Command	Description
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server retransmit	Specifies the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
show radius statistics	Displays the RADIUS statistics for accounting and authentication packets.

radius-server vsa send

To configure the network access server (NAS) to recognize and use vendor-specific attributes (VSAs), use the **radius-server vsa send** command in global configuration mode. To disable the NAS from using VSAs, use the **no** form of this command.

radius-server vsa send [**accounting**| **authentication**| **cisco-nas-port**] **[3gpp2]**

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

Syntax Description

accounting	(Optional) Limits the set of recognized VSAs to only accounting attributes.
authentication	(Optional) Limits the set of recognized VSAs to only authentication attributes.
cisco-nas-port	(Optional) Returns the Cisco NAS port VSA. **Note** Due to the IETF requirement for including NAS port information in attribute 87 (Attr87), the Cisco NAS port is obsoleted by default.
3gpp2	(Optional) Adds Third Generation Partnership Project 2 (3GPP2) Cisco VSAs to the 3GPP2 packet type.

Command Default

NAS is not configured to recognize and use VSAs.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3T	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.
12.2(33)SRA	This command was modified. The **cisco-nas-port** and **3gpp2** keywords were added to provide backward compatibility for Cisco VSAs.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Release	Modification
Cisco IOS XE Release 3.8S	This command was modified. The **accounting** and **authentication** keywords were enabled by default for NAS to use VSAs in accounting and authentication requests, respectively.

Usage Guidelines

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

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

```
"protocol : attribute separator value"
```

In the preceding example, *protocol* is a value of the Cisco protocol attribute for a particular type of authorization; *attribute* and *value* are an appropriate attribute-value (AV) pair defined in the Cisco TACACS+ specification; and *separator* is = for mandatory attributes. This solution allows the full set of features available for TACACS+ authorization to also be used for RADIUS.

For example, the following AV pair causes the Multiple Named IP Address Pools feature to be activated during IP authorization (that is, during the PPP Internet Protocol Control Protocol [IPCP] address assignment):

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

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

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

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

Examples

The following example shows how to configure the NAS to recognize and use vendor-specific accounting attributes:

```
Device(config)# 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.
show running-config all	Displays complete configuration information, including the default settings and values.

rd

To specify a route distinguisher (RD) for a VPN routing and forwarding (VRF) instance, use the **rd**command in VRF configuration mode. To remove a route distinguisher, use the **no** form of this command.

rd *route-distinguisher*

no rd *route-distinguisher*

Syntax Description

route-distinguisher	An 8-byte value to be added to an IPv4 prefix to create a VPN IPv4 prefix.

Command Default

No RD is specified.

Command Modes

VRF configuration (config-vrf)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	Support for IPv6 was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(54)SG	This command was integrated into Cisco IOS Release 12.2(54)SG.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

An RD creates routing and forwarding tables and specifies the default route distinguisher for a VPN. The RD is added to the beginning of the customer's IPv4 prefixes to change them into globally unique VPN-IPv4 prefixes.

An RD is either:

- ASN-related--Composed of an autonomous system number and an arbitrary number.
- IP-address-related--Composed of an IP address and an arbitrary number.

You can enter an RD in either of these formats:

16-bit autonomous-system-number **:** *your 32-bit number* For example, 101:3.

32-bit IP address **:** *your 16-bit number* For example, 192.168.122.15:1.

Examples

The following example shows how to configure a default RD for two VRFs. It illustrates the use of both autonomous-system-number-relative and IP-address-relative RDs:

```
Router(config)# ip vrf vrf1
Router(config-vrf)# rd 100:3
Router(config-vrf)# exit
Router(config)# ip vrf vrf2
Router(config-vrf)# rd 10.13.0.12:200
```

The following is an example of a VRF for IPv4 and IPv6 that has common policies defined in the global part of the VRF configuration:

```
vrf definition vrf2
 rd 200:1
 route-target both 200:2
!
 address-family ipv4
 exit-address-family
!
 address-family ipv6
 exit-address-family
 end
```

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
show ip vrf	Displays the set of defined VRFs and associated interfaces.
vrf definition	Configures a VRF routing table and enters VRF configuration mode.