

RADIUS Commands

This chapter contains the following sections:

- radius-server force-message-authenticator, on page 2
- radius-server host, on page 3
- radius-server key, on page 5
- radius-server retransmit, on page 6
- radius-server host source-interface, on page 7
- radius-server host source-interface-ipv6, on page 8
- radius-server timeout, on page 9
- radius-server deadtime, on page 10
- show radius-servers, on page 11
- show radius-servers key, on page 12

radius-server force-message-authenticator

Use the radius-server force-message-authenticator Global Configuration mode command to enable Message-Authenticator attribute verification for all types of RADIUS responses received from the specified RADIUS server. Use the no form of the command to restore the default setting.

Syntax

radius-server force-message-authenticator host {*ip-address* | *hostname*}

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

Parameters

- *ip-address*—Specifies the RADIUS server host IP address. The IP address can be an IPv4, IPv6 or IPv6z address.
- *hostname*—Specifies the RADIUS server host name. Translation to IPv4 addresses only is supported. (Length: 1–158 characters. Maximum label length of each part of the hostname: 63 characters)

Default Configuration

Message-Authenticator attribute verification is enabled only for RADIUS responses that are part of a RADIUS exchanges using EAP authentication.

Command Mode

Global Configuration mode

User Guidelines

Use the radius-server force-message-authenticator command to to ensure that all RADIUS responses from the specified server include the Message-Authenticator attribute (RADIUS attribute 80. If this setting is enabled, any type of RADIUS response that does not include the Message-Authenticator attribute will be silently discarded and the event will be logged. If this setting is disabled, then RADIUS responses that do not include this attribute will be discarded only if they are part of an RADIUS exchange using EAP authentication.

The command will fail if the RADIUS server specified in the host parameter was not previously configured on the device using the radius-server host command.

Example

Example 1 - The following example enables Message-Authentication attribute verification for all types of RADIUS responses received from RADIUS server 1.2.3.4.

```
switchxxxxxx(config)# radius-server force-message-authenticator host 1.2.3.4
```

Example 2 - In the following example the attempt to enable Message-Authentication attribute verification for all types of RADIUS responses received from RADIUS server 5.6.7.8 fails because RADIUS server 5.6.7.8 is not configured on the device.

```
switchxxxxxx(config)# radius-server force-message-authenticator host 5.6.7.8
Command failed since RADIUS server 5.6.7.8 was not configured on the device.
```

radius-server host

Use the **radius-server host** Global Configuration mode command to configure a RADIUS server host. Use the no form of the command to delete the specified RADIUS server host.

Syntax

radius-server host {*ip-address* | *hostname*} [**auth-port** *auth-port-number*] [**acct-port** *acct-port-number*] [**timeout** *timeout*] [**retransmit** *retries*] [**deadtime** *deadtime*] [**key** *key-string*] [**priority** *priority*] [**usage** {**login** | **dot1.x** | **all**}]

encrypted radius-server host {*ip-address* | *hostname*} [**auth-port** *auth-port-number*] [**acct-port** *acct-port-number*] [**timeout** *timeout*] [**retransmit** *retries*] [**deadtime** *deadtime*] [**key** *encrypted-key-string*] [**priority** *priority*] [**usage** {**login** | **dot1.x** | **all**}]

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

Parameters

- ***ip-address***—Specifies the RADIUS server host IP address. The IP address can be an IPv4, IPv6 or IPv6z address.
- ***hostname***—Specifies the RADIUS server host name. Translation to IPv4 addresses only is supported. (Length: 1–158 characters. Maximum label length of each part of the hostname: 63 characters)
- **auth-port** *auth-port-number*—Specifies the port number for authentication requests. If the port number is set to 0, the host is not used for authentication. (Range: 0–65535)
- **acct-port** *acct-port-number*—Port number for accounting requests. The host is not used for accountings if set to 0. If unspecified, the port number defaults to 1813.
- **timeout** *timeout*—Specifies the timeout value in seconds. (Range: 1–30)
- **retransmit** *retries*—Specifies the number of retry retransmissions (Range: 1–15)
- **deadtime** *deadtime*—Specifies the length of time in minutes during which a RADIUS server is skipped over by transaction requests. (Range: 0–2000)
- **key** *key-string*—Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. To specify an empty string, enter "". (Length: 0–128 characters). If this parameter is omitted, the globally-configured radius key will be used.
- **key** encrypted-*key-string*—Same as key-string, but the key is in encrypted format.
- **priority** *priority*—Specifies the order in which servers are used, where 0 has the highest priority. (Range: 0–65535)
- **usage** {**login** | **dot1.x** | **all**}—Specifies the RADIUS server usage type. The possible values are:

  login—Specifies that the RADIUS server is used for user login parameters authentication.

  dot1.x—Specifies that the RADIUS server is used for 802.1x port authentication.

  all—Specifies that the RADIUS server is used for user login authentication and 802.1x port authentication.

Default Configuration

The default authentication port number is 1812.

If **timeout** is not specified, the global value (set in the command) is used.

If **retransmit** is not specified, the global value (set in the command) is used.

If **key-string** is not specified, the global value (set in the command) is used.

If the **usage** keyword is not specified, the **all** argument is applied.

Command Mode

Global Configuration mode

User Guidelines

To specify multiple hosts, this command is used for each host.

Example

The following example specifies a RADIUS server host with IP address 192.168.10.1, authentication request port number 20, and a 20-second timeout period.

```
switchxxxxxx(config)# radius-server host 192.168.10.1 auth-port 20 timeout 20
```

radius-server key

Use the **radius-server key** Global Configuration mode command to set the authentication key for RADIUS communications between the device and the RADIUS daemon. Use the **no** form of this command to restore the default configuration.

Syntax

radius-server key [*key-string*]

encrypted radius-server key [*encrypted-key-string*]

no radius-server key

Parameters

- ***key-string***—Specifies the authentication and encryption key for all RADIUS communications between the device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. (Range: 0–128 characters)
- ***encrypted-key-string***—Same as the key-string parameter, but the key is in encrypted form.

Default Configuration

The key-string is an empty string.

Command Mode

Global Configuration mode

Example

The following example defines the authentication key for all RADIUS communications between the device and the RADIUS daemon.

```
switchxxxxxx(config)# radius-server key enterprise-server
```

radius-server retransmit

Use the **radius-server retransmit** Global Configuration mode command to specify the number of times the software searches the list of RADIUS server hosts. Use the no form of this command to restore the default configuration.

Syntax

radius-server retransmit *retries*

no radius-server retransmit

Parameters

- **retransmit** *retries*—Specifies the number of retry retransmissions (Range: 1–15).

Default Configuration

The software searches the list of RADIUS server hosts 3 times.

Command Mode

Global Configuration mode

Example

The following example configures the number of times the software searches all RADIUS server hosts as 5.

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

radius-server host source-interface

Use the **radius-server host source-interface** Global Configuration mode command to specify the source interface whose IPv4 address will be used as the Source IPv4 address for communication with IPv4 RADIUS servers. Use the **no** form of this command to restore the default configuration.

Syntax

radius-server host source-interface *interface-id*

no radius-server host source-interface

Parameters

- ***interface-id***—Specifies the source interface.

Default Configuration

The source IPv4 address is the IPv4 address defined on the outgoing interface and belonging to next hop IPv4 subnet.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the interface IP address belonging to next hop IPv4 subnet is applied.

If the source interface is not the outgoing interface, the minimal IPv4 address defined on the source interface is applied.

If there is no available IPv4 source address, a SYSLOG message is issued when attempting to communicate with an IPv4 RADIUS server.

OOB cannot be defined as a source interface.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# radius-server host source-interface vlan 100
```

radius-server host source-interface-ipv6

Use the **radius-server host source-interface-ipv6** Global Configuration mode command to specify the source interface whose IPv6 address will be used as the source IPv6 address for communication with IPv6 RADIUS servers. Use the **no** form of this command to restore the default configuration.

Syntax

radius-server host source-interface-ipv6 *interface-id*

no radius-server host source-interface-ipv6

Parameters

- ***interface-id***—Specifies the source interface.

Default Configuration

The IPv6 source address is the IPv6 address defined on the outgoing interface and selected in accordance with RFC6724.

Command Mode

Global Configuration mode

User Guidelines

If the source interface is the outgoing interface, the source IPv6 address is an IPv6 address defined on the interfaces and selected in accordance with RFC 6724.

If the source interface is not the outgoing interface, the source IPv6 address is the minimal IPv6 address defined on the source interface and matched to the scope of the destination IPv6 address is applied.

If there is no available source IPv6 address, a SYSLOG message is issued when attempting to communicate with an IPv6 RADIUS server.

Example

The following example configures the VLAN 10 as the source interface.

```
switchxxxxxx(config)# radius-server host source-interface-ipv6 vlan 100
```

radius-server timeout

Use the **radius-server timeout** Global Configuration mode command to set how long the device waits for a server host to reply. Use the **no** form of this command to restore the default configuration.

Syntax

radius-server timeout *timeout-seconds*

no radius-server timeout

Parameters

- **timeout** *timeout-seconds*—Specifies the timeout value in seconds. (Range: 1–30).

Default Configuration

The default timeout value is 3 seconds.

Command Mode

Global Configuration mode

Example

The following example sets the timeout interval on all RADIUS servers to 5 seconds.

```
switchxxxxxx(config)# radius-server timeout 5
```

radius-server deadtime

Use the **radius-server deadtime** Global Configuration mode command to configure how long unavailable RADIUS servers are skipped over by transaction requests. This improves RADIUS response time when servers are unavailable. Use the **no** form of this command to restore the default configuration.

Syntax

radius-server deadtime *deadtime*

no radius-server deadtime

Parameters

- ***deadtime***—Specifies the time interval in minutes during which a RADIUS server is skipped over by transaction requests. (Range: 0–2000).

Default Configuration

The default deadtime interval is 0.

Command Mode

Global Configuration mode

Example

The following example sets all RADIUS server deadtimes to 10 minutes.

```
switchxxxxxx(config)# radius-server deadtime 10
```

show radius-servers

Use the **show radius-servers** Privileged EXEC mode command to display the RADIUS server settings.

Syntax

show radius-servers

Command Mode

Privileged EXEC mode

Example

The following example displays RADIUS server settings:

```
switchxxxxxx# show radius-servers
IP address  Port Port Time                Dead    Deadtime
            Auth Acc  Out   Retransmission time     status     Priority Usage Force MA
Attribute
----------  ---- ---- ----  ------------- ------    ------     -------- -----
172.16.1.1  1812 1813  125  Global        Global     Dead        1      All         enable
172.16.1.2  1812 1813  102  8             Global     Up         2      All         disabled
Global values
--------------
TimeOut: 3
Retransmit: 3
Deadtime: 0
Source IPv4 interface: vlan 120
Source IPv6 interface: vlan 10
```

show radius-servers key

Use the **show radius-servers key** Privileged EXEC mode command to display the RADIUS server key settings.

Syntax

show radius-servers key

Command Mode

Privileged EXEC mode

Example

The following example displays RADIUS server key settings.

```
switchxxxxxx# show radius-servers key

IP address                              Key (Encrypted)
----------                              ---------------
172.16.1.1                              1238af77aaca17568f1298cced165fec
172.16.1.2                              1238af77aaca17568f12988601fcabed

Global key (Encrypted)
----------------------
1238af77aaca17568f1298bc5476ddad
```