1 RADIUS Commands

Command	Function
aaa group server radius	Configure a Remote Authentication Dial-In User Service (RADIUS) server group.
ip radius source-interface	Configure the source IP address for RADIUS packets.
ip oob	Configure an MGMT port to be used by a RADIUS server group.
ip vrf forwarding	Specify a virtual routing and forwarding (VRF) instance for a RADIUS server group.
radius data-flow-format	Configure the units of data flows and data packets to be sent to a RADIUS server.
radius dscp	Configure the differentiated services code point (DSCP) value for RADIUS packets.
radius vendor-specific extend	Enable the function of not differentiating private vendor IDs during RADIUS packet parsing.
radius vendor-specific attribute support	Enable the function of parsing private attributes of Cisco, Huawei, and Microsoft devices carried in RADIUS packets.
radius-server accounting-on enable	Enable the function of sending accounting-on packets upon device restart.
radius-server account update retransmit	Enable the function of retransmitting accounting update packets of 2nd-generation Web-authenticated users.
radius-server attribute 31	Configure the MAC address format for the Calling-Station-ID attribute of RADIUS.
radius-server attribute nas-port-id format	Configure the encapsulation format for the NAS-Port-ID attribute of RADIUS.
radius-server attribute class	Enable the function of parsing the rate limit configuration from the class attribute of RADIUS.
radius-server dead-criteria	Configure the criteria for the device to judge that a RADIUS server is unreachable.

radius-server deadtime	Configure the duration for the device to stop sending request packets to a RADIUS server when the server is unreachable.
radius-server host	Configure a RADIUS server.
radius-server key	Configure a shared key for the communication between the device and a RADIUS server.
radius-server retransmit	Configure the number of times that the device retransmits packets to a RADIUS server before confirming that the RADIUS server is unreachable.
radius-server source-port	Configure the source port for the device to send RADIUS packets.
radius-server timeout	Configure the waiting time, after which the device retransmits a RADIUS request packet.
radius-server authentication attribute	Configure whether authentication request packets carry specified attributes.
radius-server account attribute	Configure whether RADIUS accounting request packets carry specified attributes.
radius-server authentication vendor	Configure authentication request packets to carry private attributes of other vendors.
radius-server accounting-copy	Enable the function of copying and sending RADIUS accounting packets to servers in a specified server group.
radius-server account vendor	Configure RADIUS accounting request packets to carry private attributes of other vendors.
radius set qos cos	Set the quality of service (QoS) value delivered by RADIUS to the class of service (CoS) value of an interface.
radius support cui	Enable RADIUS to support the CUI attribute.
server auth-port acct-port	Configure a server for a RADIUS server group.
show radius acct statistics	Display RADIUS accounting statistics.
show radius auth statistics	Display RADIUS authentication statistics.
show radius group	Display the configuration of a RADIUS server group.
show radius parameter	Display global parameters of a RADIUS server.
show radius server	Display the configuration of a RADIUS server.
show radius vendor-specific	Display the configurations of RADIUS private

	attribute types.
show radius attribute	Display RADIUS standard attributes.
show radius-server accounting-copy	Display the configuration of copying and sending accounting packets.

1.1 aaa group server radius

Function

Run the **aaa group server radius** command to configure a Remote Authentication Dial-In User Service (RADIUS) server group.

Run the **no** form of this command to remove this configuration.

No RADIUS server group is configured by default.

Syntax

aaa group server radius *group-name*

no aaa group server radius *group-name*

Parameter Description

group-name: Name of a server group.

Caution

The name of a server group cannot be the keyword **radius** or **tacacs+**. The two keywords are the default server group names of RADIUS and TACACS+ respectively.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures an AAA server group of the RADIUS type, with the name **ss**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa group server radius ss
Hostname(config-gs-radius)#
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 ip radius source-interface

Function

Run the **ip radius source-interface** command to configure the source IP address for RADIUS packets.

Run the **no** form of this command to restore the default configuration.

The source IP address of RADIUS packets is set by the network layer by default.

Syntax

ip radius source-interface *interface-type interface-number*

no ip radius source-interface

Parameter Description

interface-type interface-number: Interface type and interface number. The first IP address of the interface is used as the source IP address of RADIUS packets.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

After this command is configured, the device uses the first IP address of the interface specified in the command as the source address of RADIUS packets. Ensure that the communication between the configured IP address and a RADIUS server is normal. Specifying the source IP address for packets to be sent to a RADIUS server can reduce the NAS information maintenance workload on the RADIUS server.

Examples

The following example configures the first IP address of interface GigabitEthernet 0/1 as the source IP address of RADIUS packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip radius source-interface gigabitethernet 0/1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 ip oob

Function

Run the **ip oob** command to configure an MGMT port to be used by a RADIUS server group.

Run the **no** form of this command to remove this configuration.

No MGMT port to be used by a RADIUS server group is configured by default.

Syntax

ip oob [**via Mgmt** *Mgmt_number*]

no ip

Parameter Description

via Mgmt *Mgmt_number*: MGMT port to be used by a RADIUS server group. MGMT 0 is used by default.

Command Modes

Server group configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example creates a server group named **ss** and sets the source interface to be used by the server group to send RADIUS packets to MGMT 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa group server radius ss
Hostname(config-gs-radius)# server 192.168.4.14
Hostname(config-gs-radius)# server 192.168.4.15
Hostname(config-gs-radius)# ip oob via mgmt 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- aaa group server radius

1.4 ip vrf forwarding

Function

Run the **ip vrf forwarding** command to specify a virtual routing and forwarding (VRF) instance for a RADIUS server group.

Run the **no** form of this command to remove this configuration.

No VRF instance is specified for a RADIUS server group by default.

Syntax

ip vrf forwarding *vrf-name*

no ip

Parameter Description

vrf-name: VRF instance used by a RADIUS server group.

Command Modes

Server group configuration mode

Default Level

14

Usage Guidelines

The VRF instance specified for a RADIUS server group must use a valid name configured using the **vrf definition** command in global configuration mode.

Examples

The following example sets the VRF instance used by a RADIUS server group named **ss** to **vrf-name**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa group server radius ss
Hostname(config-gs-radius)# server 192.168.4.12
Hostname(config-gs-radius)# server 192.168.4.13
Hostname(config-gs-radius)# ip vrf forwarding vrf-name
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- aaa group server radius

1.5 radius data-flow-format

Function

Run the **radius data-flow-format** command to configure the units of data flows and data packets to be sent to a RADIUS server.

Run the **no** form of this command to restore the default configuration.

The default units of data flows and data packets to be sent to a RADIUS server are bytes and packets respectively.

Syntax

radius data-flow-format { { **data byte** | **data giga-byte** | **data kilo-byte** | **data mega-byte** } | { **packet giga-packet** | **packet kilo-packet** | **packet mega-packet** | **packet one-packet** } } *

no radius data-flow-format

Parameter Description

data byte: Sets the unit of data flows to bytes.

data giga-byte: Sets the unit of data flows to gigabytes.

data kilo-byte: Sets the unit of data flows to kilobytes.

data mega-byte: Sets the unit of data flows to megabytes.

packet giga-packet: Sets the unit of data packets to giga-packets.

packet kilo-packet: Sets the unit of data packets to kilo-packets.

packet mega-packet: Sets the unit of data packets to mega-packets.

packet one-packet: Sets the unit of data packets to packets.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the unit of data flows to be sent to a RADIUS server to kilobytes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius data-flow-format data kilo-byte
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.6 radius dscp

Function

Run the **radius dscp** command to configure the differentiated services code point (DSCP) value for RADIUS packets.

Run the **no** form of this command to restore the default configuration.

The default DSCP value of RADIUS packets is **0**.

Syntax

radius dscp *dscp-value*

no radius dscp

Parameter Description

dscp-value: DSCP value of RADIUS packets. The value range is from 0 to 63.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

DSCP is in the type of service (ToS) field of the IP header and is used to identify the packet transmission priority. A larger DSCP value indicates a higher packet priority. The default DSCP value of RADIUS packets is **0**. You can configure the DSCP value for RADIUS packets to change the transmission priority of RADIUS packets.

Examples

The following example sets the DSCP value of RADIUS packets to **2**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius dscp 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.7 radius vendor-specific extend

Function

Run the **radius vendor-specific extend** command to enable the function of not differentiating private vendor IDs during RADIUS packet parsing.

Run the **no** form of this command to disable this feature.

The function of not differentiating private vendor IDs during RADIUS packet parsing is disabled and only Orion private vendor ID is identified by default.

Syntax

radius vendor-specific extend

no radius vendor-specific extend

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of not differentiating private vendor IDs during RADIUS packet parsing.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius vendor-specific extend
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.8 radius vendor-specific attribute support

Function

Run the **radius vendor-specific attribute support** command to enable the function of parsing private attributes of Cisco, Huawei, and Microsoft devices carried in RADIUS packets.

Run the **no** form of this command to disable this feature.

The function of parsing private attributes of Cisco, Huawei, and Microsoft devices carried in RADIUS packets is enabled by default.

Syntax

radius vendor-specific attribute support { **cisco** | **huawei** | **ms** }

no radius vendor-specific attribute support { **cisco** | **huawei** | **ms** }

Parameter Description

cisco: Supports the parsing of Cisco private attributes.

huawei: Supports the parsing of Huawei private attributes.

ms: Supports the parsing of Microsoft private attributes.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example disables the function of parsing Huawei private attributes carried in RADIUS packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no radius vendor-specific attribute support huawei
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 radius-server accounting-on enable

Function

Run the **radius-server accounting-on enable** command to enable the function of sending accounting-on packets upon device restart.

Run the **no** form of this command to disable this feature.

The function of sending accounting-on packets upon device restart is enabled by default.

Syntax

radius-server accounting-on enable

no radius-server accounting-on enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The accounting-on function is used to notify a RADIUS server of the device restart. After the device is restarted, online users are forced offline. However, the RADIUS server does not perceive the device restart and does not log off the users. As a result, the users encounter an exception when initiating re-authentication. Therefore, it is necessary to enable the accounting-on function.

Examples

The following example enables the function of sending accounting-on packets upon device restart.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no radius-server accounting-on enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.10 radius-server account update retransmit

Function

Run the **radius-server account update retransmit** command to enable the function of retransmitting accounting update packets of 2nd-generation Web-authenticated users.

Run the **no** form of this command to disable this feature.

The function of retransmitting accounting update packets of 2nd-generation Web-authenticated users is enabled by default.

Syntax

radius-server account update retransmit

no radius-server account update retransmit

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The configuration does not affect users of other authentication types.

Examples

The following example enables the function of retransmitting accounting update packets of 2nd-generation Web-authenticated users.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server account update retransmit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 radius-server attribute 31

Function

Run the **radius-server attribute 31** command to configure the MAC address format for the **Calling-Station-ID** attribute of RADIUS.

Run the **no** form of this command to restore the default configuration.

The MAC address format of the **Calling-Station-ID** attribute uses the unformatted pattern by default.

Syntax

radius-server attribute 31 mac format { **3hyphen** | **ietf** | **normal** | **unformatted** | { { **colon-split** | **dot-split** | **hyphen-split** } { **mode1** | **mode2** } [**lowercase** | **uppercase**] } }

no radius-server attribute 31 mac format

Parameter Description

3hyphen: Sets the MAC address format to 00d0-4096-3e4a.

ietf: Sets the MAC address format to the standard format specified in the Internet Engineering Task Force (IETF) standard (RFC3580). It uses hyphens (-) as the separator, for example, 00-D0-F8-33-22-AC.

normal: Sets the MAC address format to normal format, that is, dotted hexadecimal format using dots (.) as the separator, for example, 00d0.f833.22ac.

unformatted: Sets the MAC format type to unformatted pattern without separators, for example, 00d0f83322ac.

colon-split: Sets the MAC address format to a pattern using colons (:) as the separator. The final format is determined together with the **mode1** and **mode2** parameters.

dot-split: Sets the MAC address format to a pattern using dots (.) as the separator. The final format is determined together with the **mode1** and **mode2** parameters.

hyphen-split: Sets the MAC address format to a pattern using hyphens (-) as the separator. The final format is determined together with the **mode1** and **mode2** parameters.

mode1: Sets the MAC address format to a pattern using three groups with four characters in each group. It needs to be used together with **dot-split**, **colon-split**, and **hyphen-split**, for example, 00D0.F833.22AC, 00D0:F833:22AC, and 00D0-F833-22AC.

mode2: Sets the MAC address format to a pattern using six groups with two characters in each group. It needs to be used together with **dot-split**, **colon-split**, and **hyphen-split**, for example, 00.D0.F8.33.22.AC, 00:D0:F8:33:22:AC, and 00-D0-F8-33-22-AC.

lowercase: Sets the MAC address format to use lowercase letters.

uppercase: Sets the MAC address format to use uppercase letters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the uppercase/lowercase form is not specified for the MAC address format, the lowercase form is used by default.

Some RADIUS servers (mainly used for IEEE 802.1X authentication) can identify MAC addresses only in the IETF format. In this case, set the MAC address format of **Calling-Station-ID** to IETF.

Examples

The following example sets the MAC address format of the **Calling-Station-ID** attribute to IETF.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server attribute 31 mac format ietf
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 radius-server attribute nas-port-id format

Function

Run the **radius-server attribute nas-port-id format** command to configure the encapsulation format for the **NAS-Port-ID** attribute of RADIUS.

Run the **no** form of this command to restore the default configuration.

The **NAS-Port-ID** attribute of RADIUS uses the normal encapsulation format by default.

Syntax

radius-server attribute nas-port-id format { **mode1** | **normal** | **port-vid** | **qinq** }

no radius-server attribute nas-port-id format

Parameter Description

mode1: Indicates one encapsulation format of the **NAS-Port-ID** attribute of RADIUS. The format is slot = XX; subslot = XX; port = XXX; VLAN ID = XXXX. If the range of a user interface is beyond 255, this format cannot be used. Parameters in this format are described as follows:

- **slot**: Indicates the device ID. The value range is from 0 to 15.
- **subslot**: Indicates the slot ID. The value range is from 0 to 15.
- **port**: Indicates the port ID. The value range is from 0 to 255.
- **VLAN ID**: Indicates the VLAN ID. The value range is from 1 to 4094.

normal: Indicates one encapsulation format of the **NAS-Port-ID** attribute of RADIUS. The format is %Interface_name%. **Interface_name** refers to the name of a user interface. The name is displayed based on the actual length and the maximum length is 32 bytes.

port-vid: Sets the encapsulation format to port-vid. The format is %Interface%:%vid%. Parameters in the format are described as follows:

- **Interface**: Indicates the name of a user interface. The name is displayed based on the actual length and the maximum length is 32 bytes.
- **vid**: Indicates the ID of a user VLAN.

qinq: Indicates one encapsulation format of the **NAS-Port-ID** attribute of RADIUS.

Format without an inner VID: %Interface_name%.%outer_vid4%%tag%:%outer_vid%.

Format with an inner VID: %Interface_name%.%outer_vid4%%inner_vid4%:%outer_vid%-%inner_vid%.

Parameters in the format are described as follows:

- **Interface_name**: Indicates the name of a user interface. The name is displayed based on the actual length and the maximum length is 32 bytes.
- **outer_vid4**: Indicates the outer VLAN ID (it occupies four digits and spaces are filled in when there are less than four digits).
- **inner_vid4**: Indicates the inner VLAN ID (it occupies four digits and spaces are filled in when there are less than four digits).
- **tag**: Indicates a tag and the value is **0** (it occupies four digits and spaces are filled in when there are less than four digits).
- **outer_vid**: Indicates the outer VLAN ID (the number of digits is not limited, and the actual number is printed. For example, 10 is printed for VLAN 10).
- **inner_vid**: Indicates the inner VLAN ID (the number of digits is not limited, and the actual number is printed. For example, 10 is printed for VLAN 10).

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the encapsulation format of the **NAS-Port-ID** attribute of RADIUS to QinQ format.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server attribute nas-port-id format qinq
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 radius-server attribute class

Function

Run the **radius-server attribute class** command to enable the function of parsing the rate limit configuration from the **class** attribute of RADIUS.

Run the **no** form of this command to disable this feature.

The function of parsing the rate limit configuration from the **class** attribute of RADIUS is disabled by default.

Syntax

radius-server attribute class user-flow-control { **format-16bytes** | **format-32bytes** | **unit bit/s** | **unit byte/s** }}

no radius-server attribute class user-flow-control

Parameter Description

format-16bytes: Sets the format of the rate limit value parsed from the **class** attribute to 16 bytes.

format-32bytes: Sets the format of the rate limit value parsed from the **class** attribute to 32 bytes.

unit bit/s: Sets the format of the rate limit value parsed from the **class** attribute to bps.

unit byte/s: Sets the format of the rate limit value parsed from the **class** attribute to bytes/s.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of parsing the rate limit configuration from the **class** attribute of RADIUS and sets the format of the parsed rate limit value to 32 bytes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server attribute class user-flow-control format-32bytes
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 radius-server dead-criteria

Function

Run the **radius-server dead-criteria** command to configure the criteria for the device to judge that a RADIUS server is unreachable.

Run the **no** form of this command to restore the default configuration.

The criteria for judging that a RADIUS server is unreachable are that the timeout duration is **60** seconds and the consecutive timeout count is **10** by default.

Syntax

radius-server dead-criteria { **time** *timeout* | **tries** *tries-number* | **time** *timeout* **tries** *tries-number* }

no radius-server dead-criteria { **time** | **tries** | **time tries** }

Parameter Description

time *timeout*: Configures the timeout duration, in seconds. The value range is from 1 to 120. If the device fails to receive a correct response packet from a RADIUS server within the specified time, it is deemed that the RADIUS server meets the unreachability duration condition.

tries *tries-number*: Configures the consecutive timeout count. The value range is from 1 to 100. When the consecutive timeout count of request packets sent by the device to the same RADIUS server reaches the configured count, it is deemed that the RADIUS server meets the consecutive timeout count condition of unreachability.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If a RADIUS server meets both the duration condition and the consecutive request timeout count condition, it is deemed that the RADIUS server is unreachable. You can use this command to adjust the timeout duration and consecutive request timeout count.

Examples

The following example configures the criteria for judging that a RADIUS server is unreachable as follows: The timeout duration is **120** seconds and the consecutive timeout count to **20**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server dead-criteria time 120 tries 20
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 radius-server deadtime

Function

Run the **radius-server deadtime** command to configure the duration for the device to stop sending request packets to a RADIUS server when the server is unreachable.

Run the **no** form of this command to restore the default configuration.

Even if a RADIUS server is unreachable, the device still sends requests to the RADIUS server by default.

Syntax

radius-server deadtime *deadtime*

no radius-server deadtime

Parameter Description

deadtime: Duration for the device to stop sending requests to an unreachable RADIUS server, in minutes. The value range is from 1 to 1440.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If active detection is enabled for a RADIUS server on the device, the time parameter configured by the **radius-server deadtime** command does not take effect on the RADIUS server. Otherwise, if the duration in which the RADIUS server is unreachable exceeds the time specified by the **radius-server deadtime** command, the device automatically restores the RADIUS server to the reachable state.

Examples

The following example sets the duration for the device to stop sending request packets to an unreachable RADIUS server to **1** minute.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server deadtime 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 radius-server host

Function

Run the **radius-server host** command to configure a RADIUS server.

Run the **no** form of this command to remove this configuration.

No RADIUS server is configured by default.

Syntax

radius-server host [**oob** [**via Mgmt** *mgmt-number*]] { *ipv4-address* | *ipv6-address* } [**auth-port** *auth-port-number* | **acct-port** *acct-port-number*] * [**test username** *username* [**ignore-acct-port**] [**ignore-auth-port**] [**idle-time** *idle-time*]] [**key** [**0** | **7**] *text-string*]

no radius-server host [**oob** [**via Mgmt** *mgmt-number*]] { *ipv4-address* | *ipv6-address* } [**auth-port** *auth-port-number* | **acct-port** *acct-port-number*] * [**test username** *username* [**ignore-acct-port**] [**ignore-auth-port**] [**idle-time** *idle-time*]] [**key** [**0** | **7**] *text-string*]

Parameter Description

oob: Configures the device to use an MGMT port to send RADIUS packets. MGMT 0 is used for sending RADIUS packets by default.

via Mgmt *mgmt-numb*: Configures an MGMT port as the source interface for sending packets to a RADIUS server.

ipv4-address: Configures an IPv4 address for the RADIUS server.

ipv6-address: Configures an IPv6 address for the RADIUS server.

auth-port *auth-port-number*: Configures the UDP port for RADIUS authentication. The value range is from 0 to 65535 and the value **0** indicates that the server does not perform authentication.

acct-port *acct-port-number*: Configures the UDP port for RADIUS accounting. The value range is from 0 to 65535 and the value **0** indicates that the server does not perform accounting.

test username *username*: Enables the active detection function for the RADIUS server and specifies the username used in active detection.

ignore-auth-port: Disables the function of detecting the authentication port of the RADIUS server. Authentication port detection is enabled by default.

ignore-acct-port: Disables the function of detecting the accounting port of the RADIUS server. Accounting port detection is enabled by default.

idle-time *idle-minutes*: Configures the interval for the device to send test packets to a reachable RADIUS server, in minutes. The value range is from 1 to 1440 and the default value is **60**.

key [**0** | **7**] *text-string*: Configures a shared key for the server. The global shared key is used by default. You can specify the encryption type for the configured key. The value **0** indicates no encryption, **7** indicates simple encryption, and **0** is used by default.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the encryption type of a shared key is **7** and the device version is downgraded to a version that does not support the Advanced Encryption Standard (AES)-128/Secure Hash Algorithm (SHA)-256 encryption algorithm, the shared key may fail to be identified. Therefore, before the device is downgraded, set the shared key to a plaintext key or type-7 ciphertext key generated on the device of an earlier version.

A RADIUS server must be defined to implement the AAA security service by using RADIUS. You can use this command to define one or more RADIUS servers.

If a RADIUS server is not added to a RADIUS server group, the device uses the global routing table when sending RADIUS packets to the RADIUS server. Otherwise, the device uses the VRF routing table of the RADIUS server group.

Examples

The following example configures a RADIUS server in an IPv4 environment.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server host 192.168.12.1
```

The following example configures a RADIUS server in an IPv4 environment, enables active detection, sets the detection interval to **60** minutes, and disables accounting UDP port detection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server host 192.168.100.1 test username test idle-time
60 ignore-acct-port
```

The following example configures a RADIUS server in an IPv6 environment.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server host 3000::100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 radius-server key

Function

Run the **radius-server key** command to configure a shared key for the communication between the device and a RADIUS server.

Run the **no** form of this command to remove this configuration.

No shared key for the communication between the device and a RADIUS server is configured by default.

Syntax

radius-server key [**0** | **7**] *key*

no radius-server key

Parameter Description

0 | **7**: Configures the encryption type of a key. The value **0** indicates no encryption and **7** indicates simple encryption.

key: Text of a shared key.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

If the encryption type of a shared key is **7** and the device version is downgraded to a version that does not support the Advanced Encryption Standard (AES)-128/Secure Hash Algorithm (SHA)-256 encryption algorithm, the shared key may fail to be identified. Therefore, before the device is downgraded, set the shared key to a plaintext key or type-7 ciphertext key generated on the device of an earlier version.

A shared key is the basis for correct communication between the device and a RADIUS server. The same shared key must be configured on the device and a RADIUS server so that they can communicate with each other successfully.

Examples

The following example sets the shared key for the communication between the NAS and a RADIUS server to **aaa**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server key aaa
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 radius-server retransmit

Function

Run the **radius-server retransmit** command to configure the number of times that the device retransmits packets to a RADIUS server before confirming that the RADIUS server is unreachable.

Run the **no** form of this command to restore the default configuration.

The device retransmits packets to a RADIUS server three times before confirming that the RADIUS server is unreachable by default.

Syntax

radius-server retransmit *retransmit-times*

no radius-server retransmit

Parameter Description

retransmit-times: Packet retransmission count before the device confirms that a RADIUS server is unreachable. The value range is from 0 to 100 and the value **0** indicates no retransmission.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The prerequisite for AAA to use the next user authentication method is that the current security server used for authentication does not respond. The criteria for the device to judge that a security server does not respond are that the security server does not respond within the duration, in which the device retransmits RADIUS packets for a specified number of times. There is a timeout interval between two consecutive retransmissions.

Examples

The following example sets the number of times that the device retransmits packets to a RADIUS server before confirming that the RADIUS server is unreachable to 4.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server retransmit 4
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 radius-server source-port

Function

Run the **radius-server source-port** command to configure the source port for the device to send RADIUS packets.

Run the **no** form of this command to restore the default configuration.

The source port used by the device to send RADIUS packets is a random port by default.

Syntax

radius-server source-port *source-port*

no radius-server source-port

Parameter Description

source-port: Source port used by the device to send RADIUS packets. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The source port used by the device to send RADIUS packets is a random port by default. You can run this command to specify the source port.

Examples

The following example sets the source port for the device to send RADIUS packets to **10000**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server source-port 10000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 radius-server timeout

Function

Run the **radius-server timeout** command to configure the waiting time, after which the device retransmits a RADIUS request packet.

Run the **no** form of this command to restore the default configuration.

The default waiting time before the retransmission of a RADIUS packet is **5** seconds.

Syntax

radius-server timeout *timeout*

no radius-server timeout

Parameter Description

timeout: Response timeout duration of a security server, in seconds. The value range is from 1 to 1000.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the waiting time, after which the device retransmits a RADIUS request packet, to **10** seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server timeout 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 radius-server authentication attribute

Function

Run the **radius-server authentication attribute** command to configure whether authentication request packets carry specified attributes.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Whether RADIUS authentication request packets carry specified attributes is consistent with the stipulation in the RFC standard by default.

Syntax

radius-server authentication attribute *type* { **package** | **unpackage** }

no radius-server authentication attribute *type* { **package** | **unpackage** }

default radius-server authentication attribute *type* { **package** | **unpackage** }

Parameter Description

type: Type of a RADIUS attribute. The value range is from 1 to 255.

package: Indicates that RADIUS authentication request packets carry specified attributes.

unpackage: Indicates that RADIUS authentication request packets do not carry specified attributes.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures RADIUS authentication request packets not to carry attribute 87.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server authentication attribute 87 unpackage
```

Related Commands

N/A

1.22 radius-server account attribute

Function

Run the **radius-server account attribute** command to configure whether RADIUS accounting request packets carry specified attributes.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Whether RADIUS accounting request packets carry specified attributes is consistent with the stipulation in the RFC standard by default.

Syntax

radius-server account attribute *type* { **package | unpackage** }

no radius-server account attribute *type* { **package | unpackage** }

default radius-server account attribute *type* { **package | unpackage** }

Parameter Description

type: Type of a RADIUS attribute. The value range is from 1 to 255.

package: Indicates that RADIUS accounting request packets carry specified attributes.

unpackage: Indicates that RADIUS accounting request packets do not carry specified attributes.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures RADIUS accounting request packets not to carry attribute 87.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server account attribute 87 unpackage
```

Related Commands

N/A

1.23 radius-server authentication vendor

Function

Run the **radius-server authentication vendor** command to configure authentication request packets to carry private attributes of other vendors.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Authentication request packets do not carry private attributes of other vendors by default.

Syntax

radius-server authentication vendor { **cisco | cmcc** | **microsoft** } **package**

no radius-server authentication vendor { **cisco | cmcc** | **microsoft** } **package**

default radius-server authentication vendor { **cisco | cmcc** | **microsoft** } **package**

Parameter Description

cisco: Indicates that Cisco private attributes are carried.

cmcc: Indicates that CMCC private attributes are carried.

microsoft: Indicates that Microsoft private attributes are carried.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures authentication request packets to carry CMCC private attributes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server authentication vendor cmcc package
```

Related Commands

N/A

1.24 radius-server accounting-copy

Function

Run the **radius-server accounting-copy** command to enable the function of copying and sending RADIUS accounting packets to servers in a specified server group.

Run the **no** form of this command to remove this configuration and restore the default configuration.

The function of copying and sending RADIUS accounting packets is disabled by default.

Syntax

radius-server accounting-copy *group*

no radius-server accounting-copy *group*

Parameter Description

group: Server group, to which accounting packets are to be sent.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables the function of copying and sending RADIUS accounting packets to servers in a server group named **cpy-grp**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# radius-server accounting-copy cpy-grp
```

Related Commands

N/A

1.25 radius-server account vendor

Function

Run the **radius-server account vendor** command to configure RADIUS accounting request packets to carry private attributes of other vendors.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

Accounting request packets do not carry private attributes of other vendors by default.

Syntax

radius-server account vendor { **cisco | cmcc** | **microsoft** } **package**

no radius-server account vendor { **cisco | cmcc** | **microsoft** } **package**

default radius-server account vendor { **cisco | cmcc** | **microsoft** } **package**

Parameter Description

cisco: Sets the vendor type to Cisco.

cmcc: Sets the vendor type to CMCC.

microsoft: Sets the vendor type to Microsoft.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures RADIUS accounting request packets to carry CMCC private attributes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius-server account vendor cmcc package
```

Related Commands

N/A

1.26 radius set qos cos

Function

Run the **radius set qos cos** command to set the quality of service (QoS) value delivered by RADIUS to the class of service (CoS) value of an interface.

Run the **no** form of this command to remove this configuration and restore the default configuration.

The QoS value delivered by RADIUS is the DSCP value by default.

Syntax

radius set qos cos

no radius set qos cos

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the QoS value delivered by RADIUS to the CoS value of an interface.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius set qos cos
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.27 radius support cui

Function

Run the **radius support cui** command to enable RADIUS to support the CUI attribute.

Run the **no** form of this command to disable this feature.

The function of supporting the CUI attribute by RADIUS is disabled by default.

Syntax

radius support cui

no radius support cui

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example enables RADIUS to support the CUI attribute.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# radius support cui
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.28 server auth-port acct-port

Function

Run the **server auth-port acct-port** command to configure a server for a RADIUS server group.

Run the **no** form of this command to remove this configuration.

No server is configured for a RADIUS server group by default.

Syntax

server { *ipv4-address* | *ipv6-address* } [**acct-port** *acct-port* | **auth-port** *auth-port*] *

no server { *ipv4-address* | *ipv6-address* } [**acct-port** *acct-port* | **auth-port** *auth-port*] *

Parameter Description

Ipv4-address: IPv4 address of a server.

Ipv6-address: IPv6 address of a server.

acct-port *acct-port*: Configures the accounting port ID for the server. The value range is from 1 to 65535, and the default value is **1813**.

auth-port *auth-port*: Configures the authentication port ID for the server. The value range is from 1 to 65535, and the default value is **1812**.

Command Modes

Server group configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example adds a server with the IP address 192.168.4.12 to a server group named **ss**, sets the authentication port ID of the server to 10000, and the accounting port ID to 10001.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa group server radius ss
Hostname(config-gs-radius)# server 192.168.4.12 acct-port 10000 auth-port 10001
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **radius-server deadtime**

1.29 show radius acct statistics

Function

Run the **show radius acct statistics** command to display RADIUS accounting statistics.

Syntax

show radius acct statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays RADIUS accounting statistics.

```
Hostname> enable
Hostname# show radius acct statistics
Accounting Servers:
Server Index..................................... 1
Server Address................................... 192.168.1.1
Server Port...................................... 1813
Msg Round Trip Time.............................. 0 (msec)
First Requests................................... 1
Retry Requests................................... 1
Accounting Responses............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 1
```

Table 1-1Output Fields of the show radius radius acct statistics Command

Field	Description
Accounting Servers	Accounting server
Server Index	Server index
Server Address	IP address of the server
Server Port	Server port
Msg Round Trip Time	Duration from the time that an access request is sent to the server to the time an

Field	Description
	access response is received from the server
First Requests	Number of times that the first request is sent to the server
Retry Requests	Packet transmission count
Accounting Responses	Number of times that accounting response packets are received
Malformed Msgs	Number of RADIUS Access-Response error packets received from the server
Bad Authenticator Msgs	Number of packets with verification errors
Pending Requests	Number of RADIUS access request packets sent to the server, for which no timeout occurs and no response is received ● The value of this variable increases when an access request is sent. ● The value of this variable decreases when an access acceptance, access denial, access challenge, timeout, or retransmission message is received.

Notifications

N/A

Platform Description

N/A

1.30 show radius auth statistics

Function

Run the **show radius auth statistics** command to display RADIUS authentication statistics.

Syntax

show radius auth statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays RADIUS authentication statistics.

```
Hostname> enable
Hostname# show radius auth statistics
Authentication Servers:
Server Index..................................... 1
Server Address................................... 192.168.1.1
Server Port...................................... 1812
Msg Round Trip Time.............................. 0 (msec)
First Requests................................... 0
Retry Requests................................... 0
Accept Responses................................. 0
Reject Responses................................. 0
Challenge Responses.............................. 0
Malformed Msgs................................... 0
Bad Authenticator Msgs........................... 0
Pending Requests................................. 0
Timeout Requests................................. 0
Unknowntype Msgs................................. 0
Other Drops...................................... 0
```

Table 1-1Output Fields of the show radius radius auth statistics Command

Field	Description
Authentication Servers	Authentication server
Server Index	Server index
Server Address	Server address
Server Port	Server port ID
Msg Round Trip Time	Duration from the time that an access request is sent to the server to the time an access response is received from the server
First Requests	Number of times that the first request is sent
Retry Requests	Retransmission count
Accept Responses	Number of times that the Access-accept message is received
Reject Responses	Number of times that the Reject message is received
Challenge Responses	Number of times that the Challenge response message is received
Malformed Msgs	Number of RADIUS Access-Response error packets received from the server
Bad Authenticator Msgs	Number of packets with verification errors
Pending Requests	Number of RADIUS access request packets sent to the server, for which no

Field	Description
	timeout occurs and no response is received ● The value of this variable increases when an access request is sent. ● The value of this variable decreases when an access acceptance, access denial, access challenge, timeout, or retransmission message is received.
Timeout Requests	Number of timeout request times
Unknowntype Msgs	Number of packets of the unknown type
Other Drops	Number of other discarded packets

Notifications

N/A

Platform Description

N/A

1.31 show radius group

Function

Run the **show radius group** command to display the configuration of a RADIUS server group.

Syntax

show radius group

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration of a RADIUS server group.

```
Hostname> enable
Hostname# show radius group
==========Radius group radius==========
Vrf:not-set
```

```
Server:192.168.1.1
  Server key:aaaa
  Authentication port:1812
  Accounting port:1813
  State:Active
```

Table 1-1Output Fields of the show radius group Command

Field	Description
Vrf	VRF instance
Server	Server address
Server key	Server key
Authentication port	Authentication port
Accounting port	Accounting port
State	Server status

Notifications

N/A

Platform Description

N/A

1.32 show radius parameter

Function

Run the **show radius parameter** command to display global parameters of a RADIUS server.

Syntax

show radius parameter

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays global parameters of a RADIUS server.

```
Hostname> enable
Hostname# show radius parameter
Server Timout:   5 Seconds
Server Deadtime: 0 Minutes
Server Retries:  3
Server Dead Critera:
Time:        10 Seconds
Tries:       10
```

Table 1-1 Output Fields of the show radius parameter Command

Field	Description
Server Timout	Waiting time prior to request retransmission
Server Deadtime	Duration for the device to stop sending request packets to an unreachable RADIUS server
Server Retries	Number of times that the device sends requests consecutively before confirming that a RADIUS server is unreachable
Server Dead Criteria	Criteria for judging that a RADIUS server is unreachable
Time	If the device fails to receive a correct response packet from a RADIUS server within the time, it is judged that the RADIUS server meets the unreachability duration condition.
Tries	When the number of times that the device sends a request packet to the RADIUS server consecutively reaches the configured value, it is judged that the RADIUS server meets the consecutive timeout count condition of unreachability.

Notifications

N/A

Platform Description

N/A

1.33 show radius server

Function

Run the **show radius server** command to display the configuration of a RADIUS server.

Syntax

show radius server

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration of a RADIUS server.

```
Hostname> enable
Hostname# show radius server
Server IP:    192.168.4.12
Accounting  Port:  23
Authen  Port:     77
Test Username:    test
Test Idle Time:   10 Minutes
Test Ports:        Authen
Server State:     Active
    Current duration 765s, previous duration 0s
Dead: total time 0s, count 0
Statistics:
Authen: request 15, timeouts 1
Author: request 0, timeouts 0
Account: request 0, timeouts 0
Server IP:    192.168.4.13
Accounting Port:  45
Authen  Port:     74
Test Username:    <Not Configured>
Test Idle Time:   60 Minutes
Test Ports:        Authen and Accounting
Server State:     Active
Current duration 765s, previous duration 0s
Dead: total time 0s, count 0
Statistics:
Authen: request 0, timeouts 0
Author: request 0, timeouts 0
Account: request 20, timeouts 0
```

Table 1-1Output Fields of the show radius server Command

Field	Description
Server IP	Server IP address
Accounting Port	Accounting port
Authen Port	Authentication port
Test Username	Username used for active detection
Test Idle Time	Interval for sending test packets to a reachable RADIUS server
Test Ports	Port for sending test packets
Server State	Server status
Dead	Total duration in which the server is unreachable and number of times that the server is unreachable
Statistics	Statistical data
Authen	Number of authentication requests
Author	Number of authorization requests
Account	Number of accounting requests
Server IP	Server IP address
Accounting Port	Accounting port
Authen Port	Authentication port
Test Username	Username used for active detection
Test Idle Time	Interval for sending test packets to a reachable RADIUS server
Test Ports	Port for sending test packets
Server State	Server status

Notifications

N/A

Platform Description

N/A

1.34 show radius vendor-specific

Function

Run the **show radius vendor-specific** command to display the configurations of RADIUS private attribute types.

Syntax

show radius vendor-specific

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays configurations of RADIUS private attribute types.

```
Hostname> enable
Hostname# show radius vendor-specific
id    vendor-specific      type-value
-------------
1     max-down-rate        1
2     port-priority        2
3     user-ip              3
4     VLAN-id              4
5     last-supplicant-vers 5
      ion
6     net-ip               6
7     user-name            7
8     password             8
9     file-directory       9
10    file-count           10
11    file-name-0          11
12    file-name-1          12
13    file-name-2          13
14    file-name-3          14
15    file-name-4          15
16    max-up-rate          16
17    current-supplicant-v 17
      ersion
```

```
18    flux-max-high32      18
19    flux-max-low32       19
20    proxy-avoid          20
21    dialup-avoid         21
22    ip-privilege         22
23    login-privilege      42
26    ipv6-multicast-addre 79
      ss
27    ipv4-multicast-addre 87
      ss
```

Table 1-1Output Fields of the show radius vendor-specific Command

Field	Description
id	Serial number
vendor-specific	Private attribute meaning
type-value	ID of a private attribute

Notifications

N/A

Platform Description

N/A

1.35 show radius attribute

Function

Run the **show radius attribute** command to display RADIUS standard attributes.

Syntax

show radius attribute

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays RADIUS standard attributes.

```
Hostname> enable
Hostname# show radius attribute
type          implicate
----          ---------
   1.........User-Name
   2.........User-Password
   3.........Chap-Password
   4.........NAS-Ip-Addr
   5.........Nas-Ip-Port
   6.........Service-Type
   7.........Framed-Protocol
   8.........Frame-Ip-Address
   9.........Framed-Ip-Mask
  10.........Framed-Routing
  11.........Filter-Id
  12.........Framed-Mtu
  13.........Framed-Compress
  14.........Login-Ip-Host
  15.........Login-Service
  16.........Login-Tcp-Port
  18.........Reply-Message
  19.........Callback-Num
  20.........Callback-Id
  22.........Framed-Route
  23.........Framed-IPX-Network
  24.........State
  25.........Class
  26.........Vendor-Specific
  27.........Session-Timeout
  28.........Idle-Timeout
  29.........Termination-Action
  30.........Called-Station-Id
  31.........Calling-Station-Id
  32.........Nas-Id
  33.........Proxy-State
  34.........Login-LAT-Service
  35.........Login-LAT-Node
  36.........Login-LAT-Group
  37.........Framed-AppleTalk-Link
  38.........Framed-AppleTalk-Net
  39.........Framed-AppleTalk-Zone
  40.........Acct-Status-Type
  41.........Acct-Delay-Time
```

```
 42.........Acct-Input-Octets
 43.........Acct-Output-Octets
 44.........Acct-Session-Id
 45.........Acct-Authentic
 46.........Acct-Session-Time
 47.........Acct-Input-Packet
 48.........Acct-Output-Packet
 49.........Acct-Terminate-Cause
 50.........Acct-Multi-Session-ID
 51.........Acct-Link-Count
 52.........Acct-Input-Gigawords
 53.........Acct-Output-Gigawords
 60.........Chap-Challenge
 61.........Nas-Port-Type
 62.........Port-Limit
 63.........Login-Lat-Port
 64.........Tunnel-Type
 65.........Tunnel-Medium-Type
 66.........Tunnel-Client-EndPoint
 67.........Tunnel-Service-EndPoint
 79.........eap msg
 80.........Message-Authenticator
 81.........group id
 85.........Acct-Interim-Interval
 87.........Nas-Port-Id
 89.........cui
 95.........Nas-Ipv6-Addr
 96.........Framed-Interface-Id
 97.........Framed-Ipv6-Prefix
 98.........Login-Ipv6-Host
 99.........Framed-Ipv6-Route
100.........Framed-Ipv6-Pool
168.........Framed-Ipv6-Addr
```

Table 1-1Output Fields of the show radius attribute Command

Field	Description
type	Serial number
implicate	Meaning of a standard attribute

Notifications

N/A

Platform Description

N/A

1.36 show radius-server accounting-copy

Function

Run the **show radius-server accounting-copy** command to display the configuration of copying and sending accounting packets.

Syntax

show radius-server accounting-copy

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the configuration of copying and sending accounting packets.

```
Hostname> enable
Hostname# show radius-server group-attribute
```

Notifications

N/A

Platform Description

N/A