

1 TACACS Commands

Command	Function
<u>aaa group server tacacs+</u>	Configure a Terminal Access Controller Access Control System Plus (TACACS+) server group.
<u>ip tacacs source-interface</u>	Configure the source address for TACACS+ packets.
<u>ip oob</u>	Configure an MGMT port to be used by a TACACS+ server group.
<u>ip vrf forwarding</u>	Specify a VRF instance for a TACACS+ server group.
<u>server</u>	Add a server to a TACACS+ server group.
<u>nas-ip</u>	Enable the function of carrying the nas-ip attribute in packets.
<u>show tacacs</u>	Display the interaction between the device and each TACACS+ server.
<u>tacacs-server host</u>	Configure a TACACS+ server.
<u>tacacs-server key</u>	Configure a shared key for the communication between a network access server (NAS) and a TACACS+ server.
<u>tacacs-server timeout</u>	Configure the global timeout duration for a TACACS+ server in the communication between the device and the TACACS+ server.
<u>tacacs-server dead-criteria</u>	Configure the criteria for the device to judge that a TACACS+ server is unreachable.
<u>tacacs-server deadtime</u>	Configure the duration for the device to stop sending request packets to an unreachable TACACS+ server.

1.1 aaa group server tacacs+

Function

Run the **aaa group server tacacs+** command to configure a Terminal Access Controller Access Control System Plus (TACACS+) server group.

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

No TACACS+ server group is configured by default.

Syntax

```
aaa group server tacacs+ group-name
```

```
no aaa group server tacacs+ group-name
```

Parameter Description

group-name: Name of a TACACS+ server group. The value is a string of 1 to 63 characters. The name cannot be set to the default name **radius** or **tacacs+**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can group TACACS+ servers so that authentication, authorization, and accounting can be completed by different server groups.

Examples

The following example configures a TACACS+ server group named **tac1**, and adds a TACACS+ server with the IP address 1.1.1.1 to the server group.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa group server tacacs+ tac1
Hostname(config-gs-tacacs)# server 1.1.1.1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.2 ip tacacs source-interface

Function

Run the **ip tacacs source-interface** command to configure the source address for TACACS+ packets.

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

No source address is configured for TACACS+ packets and the address is set by the network layer by default.

Syntax

ip tacacs source-interface *interface-type interface-number*

no ip tacacs source-interface *interface-type interface-number*

Parameter Description

interface-type interface-number: Interface type and interface number.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You can run this command to configure the source IP address for TACACS+ packets to be sent to a TACACS+ server, to reduce the network access server (NAS) information maintenance workload on the TACACS+ server. This command uses the first IP address of a specified interface as the source address of TACACS+ packets. If a specified interface belongs to a virtual routing and forwarding (VRF) instance, routes in the VRF instance are used to send packets.

Examples

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

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip tacacs 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 TACACS+ server group.

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

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

Syntax

```
ip oob [ via Mgmt mgmt-number ]
```

```
no ip
```

Parameter Description

via Mgmt mgmt-number: Configures the number of an MGMT port to be used. MGMT 0 is used by default.

Command Modes

TACACS+ server group configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the MGMT port to be used by a TACACS+ server group named **ss** to MGMT 0.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa group server tacacs+ ss
Hostname(config-gs-tacacs)# server 192.168.1.2
Hostname(config-gs-tacacs)# ip oob via mgmt 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 ip vrf forwarding

Function

Run the **ip vrf forwarding** command to specify a VRF instance for a TACACS+ server group.

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

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

Syntax

```
ip vrf forwarding vrf-name
```

```
no ip
```

Parameter Description

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

Command Modes

TACACS+ server group configuration mode

Default Level

14

Usage Guidelines

The VRF instance specified for a TACACS+ 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 TACACS+ server group to **vrf-name**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa group server tacacs+ ss
Hostname(config-gs-tacacs+)# server 192.168.1.2
Hostname(config-gs-tacacs+)# ip vrf forwarding vrf-name
```

Notifications

If the name of a specified VRF instance exceeds the length limit, the following notification will be displayed:

```
Name is too long
```

If a specified VRF instance is not configured, the following notification will be displayed:

```
Invalid vrf
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **vrf definition** (IP routing/VRF)

1.5 server

Function

Run the **server** command to add a server to a TACACS+ server group.

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

No server is added to a TACACS+ server group by default.

Syntax

```
server { ipv4-address | ipv6-address }
```

```
no server { ipv4-address | ipv6-address }
```

Parameter Description

ipv4-address: IPv4 address of a server.

ipv6-address: IPv6 address of a server.

Command Modes

TACACS+ server group configuration mode

Default Level

14

Usage Guidelines

If multiple servers are added to one server group, when one server does not respond, the device continues to send a TACACS+ request to the next server in the server group.

Examples

The following example configures a TACACS+ server group named **tac1**, and adds a TACACS+ server with the IP address 192.168.1.2 to the server group.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa group server tacacs+ tac1
Hostname(config-gs-tacacs)# server 192.168.1.2
```

Notifications

When a server is added to a server group but the server is not configured, the following notification will be displayed:

```
Warning: Server 1.1.1.1 is not defined.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- [aaa group server tacacs+](#)

1.6 nas-ip

Function

Run the **nas-ip** command to enable the function of carrying the **nas-ip** attribute in packets.

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

Packets do not carry the **nas-ip** attribute by default.

Syntax

```
nas-ip { ipv4-address | ipv6-address }
```

```
no nas-ip { ipv4-address | ipv6-address }
```

Parameter Description

ipv4-address: **nas-ip** attribute value of an IPv4 address.

ipv6-address: **nas-ip** attribute value of an IPv6 address.

Command Modes

TACACS+ server group configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures a TACACS+ server group named **tac1** and enables the function of carrying the **nas-ip** attribute in packets for the server group.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# aaa group server tacacs+ tac1
Hostname(config-gs-tacacs)# nas-ip 192.168.197.215
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [aaa group server tacacs+](#)

1.7 show tacacs**Function**

Run the **show tacacs** command to display the interaction between the device and each TACACS+ server.

Syntax

```
show tacacs
```

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 interaction between the device and each TACACS+ server.

```

Hostname> enable
Hostname# show tacacs

Tacacs+ Server : 172.19.192.80/49
Socket Opens: 0
Socket Closes: 0
Total Packets Sent: 0
Total Packets Recv: 0
Reference Count: 0

```

Table 1-1 Output Fields of the show tacacs Command

Field	Description
Tacacs+ Server	Address of a TACACS+ server
Socket Opens	Number of established socket connections
Socket Closes	Number of released socket connections
Total Packets Sent	Number of sent packets

Field	Description
Total Packets Recv	Number of received packets
Reference Count	Server reference count

Notifications

N/A

Platform Description

N/A

1.8 tacacs-server host

Function

Run the **tacacs-server host** command to configure a TACACS+ server.

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

No TACACS+ server is configured by default.

Syntax

```
tacacs-server host [ oob [ via Mgmt mgmt-number ] ] { ipv4-address | ipv6-address } [ port port-number ] [ test username username ] [ idle-time idle-time ] [ timeout timeout ] [ key [ 0 | 7 ] key ]
no tacacs-server host [ oob [ via Mgmt mgmt-number ] ] { ipv4-address | ipv6-address }
```

Parameter Description

oob: Uses an MGMT port for communication. If this parameter is not specified, a non-MGMT port is used for communication.

via Mgmt *mgmt-number*: Specifies an MGMT port. If this parameter is not specified, MGMT 0 is used.

ipv4-address: IPv4 address of a TACACS+ server.

ipv6-address: IPv6 address of a TACACS+ server.

port *port-number*: Configures a TCP port for TACACS+ communication. The value range is from 1 to 65535, and the default value is **49**.

test username *username*: Configures a username used for detection. The value is a string of 1 to 63 characters.

idle-time *idle-time*: Configures the detection interval, in minutes. The value range is from 1 to 1440 and the default value is **60**.

timeout *timeout*: Configures the communication timeout duration of a TACACS+ server, in seconds. The value range is from 1 to 1000. If this parameter is not specified, the global timeout duration is used.

key [**0** | **7**] *key*: Configures a shared key for the server. You can specify the encryption type for the configured key. The value **0** indicates no encryption and **7** indicates simple encryption. The value **0** is used by default. If this parameter is not specified, the global shared key is used.

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.

Examples

The following example configures a TACACS+ server with the IPv4 address 192.168.12.1.

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

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.9 tacacs-server key

Function

Run the **tacacs-server key** command to configure a shared key for the communication between a network access server (NAS) and a TACACS+ server.

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

No shared key for the communication between a NAS and a TACACS+ server is configured by default.

Syntax

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

no tacacs-server key

Parameter Description

0 | **7**: Configures the encryption type of a key. The value **0** indicates no encryption and **7** indicates simple encryption. If this parameter is not specified, no encryption is adopted.

key: Text of a shared key. The value is a string of 1 to 128 characters.

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 AES-128/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.

This command is used to configure a global shared key. You can use the **key** field in the [tacacs-server host](#) command to specify different keys for servers.

Examples

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

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

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [tacacs-server host](#)

1.10 tacacs-server timeout

Function

Run the **tacacs-server timeout** command to configure the global timeout duration for a TACACS+ server in the communication between the device and the TACACS+ server.

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

The default timeout duration of a TACACS+ server is **5** seconds in the communication between the device and the TACACS+ server.

Syntax

tacacs-server timeout *timeout*

no tacacs-server timeout**Parameter Description**

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

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command is used to configure the global server response timeout duration. You can use the **timeout** field in the [tacacs-server host](#) command to specify different timeout duration values for servers.

Examples

The following example sets the global timeout duration to **10** seconds for a TACACS+ server in the communication between the device and the TACACS+ server.

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

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- [tacacs-server host](#)

1.11 tacacs-server dead-criteria

Function

Run the **tacacs-server dead-criteria** command to configure the criteria for the device to judge that a TACACS+ server is unreachable.

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

The criteria for the device to judge that a TACACS+ server is unreachable are that the server timeout duration is **60** seconds and the consecutive timeout count is **10** by default.

Syntax

```
tacacs-server dead-criteria { time timeout tries tries-number | time timeout | tries tries-number }
no tacacs-server dead-criteria { time tries | time | tries }
```

Parameter Description

time *timeout*: Configures the timeout duration to judge that a security server is unreachable, in seconds. The value range is from 1 to 120.

tries *tries-number*: Configures the consecutive timeout count to judge that a security server is unreachable. The value range is from 1 to 100.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

It is judged that a TACACS+ server is unreachable only when both conditions below are met:

- The device fails to receive a correct response packet from the TACACS+ server within the specified timeout period.
- The consecutive transmission count of a request packet sent by the device to the same TACACS+ server reaches the specified timeout count.

Examples

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

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

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 tacacs-server deadtime

Function

Run the **tacacs-server deadtime** command to configure the duration for the device to stop sending request packets to an unreachable TACACS+ server.

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

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

Syntax

tacacs-server *deadtime* *deadtime*

no tacacs-server *deadtime*

Parameter Description

deadtime: Duration for the device to stop sending requests to an unreachable TACACS+ 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 TACACS+ server on the device, the time parameter configured by the command does not take effect on the TACACS+ server. Otherwise, if the duration in which the TACACS+ server is unreachable exceeds the time specified by the command, the device automatically restores the TACACS+ server to the reachable state.

Examples

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

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

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A